PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-078520
(43)Date of publication of application : 14.03.2003

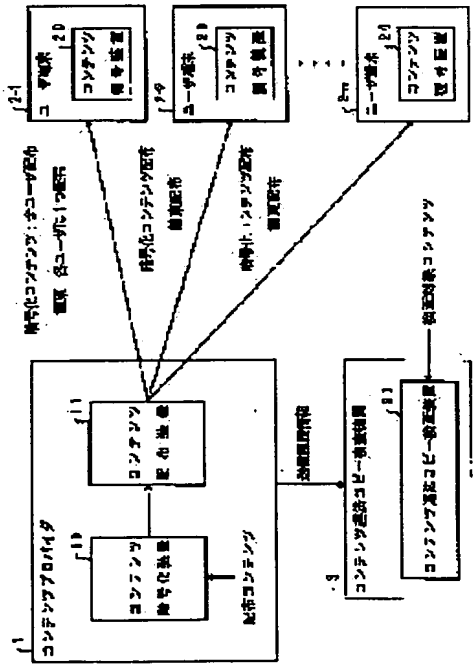
(51)Int.Cl. H04L 9/16
G09C 5/00
H04L 9/08
H04N 7/08
H04N 7/081
// H04N 7/167

(21)Application number : 2001-269623
(22)Date of filing : 06.09.2001

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : FUJII HIROSHI
YASUDA HIROSHI

(54) CONTENTS ENCODING METHOD AND DEVICE, CONTENTS DECODING METHOD AND DEVICE, CONTENTS DISTRIBUTING METHOD AND DEVICE, CONTENTS ILLEGAL COPY CHECKING METHOD AND DEVICE, CONTENTS ENCRYPTING PROGRAM AND ITS PROGRAM RECORDING MEDIUM, CONTENTS DECODING PROGRAM AND ITS PROGRAM RECORDING MEDIUM, CONTENTS DISTRIBUTING PROGRAM AND ITS PROGRAM RECORDING MEDIUM, AND CONTENTS ILLEGAL COPY CHECKING PROGRAM AND ITS PROGRAM RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a technology for allowing a user side to efficiently embed user information in contents by using an electronic watermark, and for allowing a provider side to prevent the illegal cancel of the embodiment of electronic watermark information or the embodiment of any false electronic watermark information at the same time.
SOLUTION: Contents are divided into a plurality of parts, and a plurality of electronic watermarks are prepared for those respective divided parts, and the electronic watermark for each user is acquired by combining the values of the electronic watermarks of the extracted divided parts. Thus, it is possible for the user side to realize configuration that the electronic watermark information specific to the user is embedded in the contents, and it is possible for a provider side to actually control the electronic watermark information to be embedded and the embedding processing. Thus, it is possible to prevent the illegal cancel of the embodiment of the electronic watermark information or the embodiment of any false electronic watermark information at the user side.



LEGAL STATUS
[Date of request for examination] 08.10.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－78520
（P2003－78520A）
(43)公開日　平成15年３月14日(2003.3.14)

(51)Int.Cl.'		識別記号	FI			テーマコード'(参考)
H04L	9/16		G09C	5/00		5C063
G09C	5/00		H04L	9/00	643	5C064
H04L	9/08				601B	5J104
H04N	7/08		H04N	7/08	Z	
	7/081			7/167	Z	

審査請求　未請求　請求項の数26　ＯＬ　（全 21 頁）　最終頁に続く

(21)出願番号　特願2001－269623(P2001－269623)

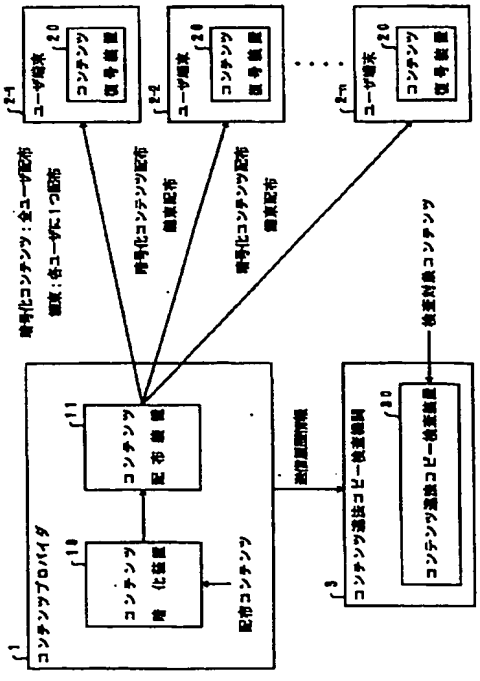
(22)出願日　平成13年９月６日(2001.9.6)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　藤井　寛
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　安田　浩
神奈川県横浜市栄区本郷台２丁目27番20号
(74)代理人　100087848
弁理士　小笠原　吉義　（外２名）

最終頁に続く

(54)【発明の名称】　コンテンツ暗号化方法及び装置と、コンテンツ復号方法及び装置と、コンテンツ配布方法及び装置と、コンテンツ違法コピー検査方法及び装置と、コンテンツ暗号化プログラム及びそのプログ

(57)【要約】
【課題】本発明は、利用者側で電子透かしを使って利用者情報をコンテンツへ効率よく埋め込みながら、電子透かし情報の埋め込みの不正なキャンセルや、偽の電子透かし情報の埋め込みを防止できるようにする技術の提供を目的とする。
【解決手段】コンテンツを複数の部分に分割して、それぞれの分割部分に対して複数の電子透かしを用意し、個々のユーザに対する電子透かしを、抽出された分割部分の電子透かしの値の組み合わせとするという構成を採る。これにより、ユーザ側で、ユーザに固有な電子透かし情報をコンテンツに埋め込むという形態をとりつつ、そのとき埋め込む電子透かし情報とその埋め込み処理とについては、実際には提供側で制御するようにしており、これにより、ユーザ側で、電子透かし情報の埋め込みを不正にキャンセルしたり、偽の電子透かし情報が埋め込まれることを防止できるようになる。



【特許請求の範囲】
【請求項１】　コンテンツに電子透かし情報を埋め込んで暗号化するコンテンツ暗号化方法において、
コンテンツを複数の部分に分割する過程と、
上記分割した部分の全て又は一部を処理対象として、処理対象の分割部分のそれぞれに対して、複数の異なる電子透かし情報を埋め込む過程と、
上記電子透かし情報の埋め込まれた分割部分及びその埋め込みの行われなかった分割部分を、別々の暗号鍵を使って暗号化する過程とを備えることを、
特徴とするコンテンツ暗号化方法。
【請求項２】　請求項１に記載のコンテンツ暗号化方法において、
上記電子透かし情報を埋め込む過程では、上記処理対象とならなかった分割部分については、電子透かし情報を埋め込まないように処理することを、
特徴とするコンテンツ暗号化方法。
【請求項３】　請求項１に記載のコンテンツ暗号化方法において、
上記電子透かし情報を埋め込む過程では、上記処理対象とならなかった分割部分については、固定的となる特定の電子透かし情報を埋め込むように処理することを、
特徴とするコンテンツ暗号化方法。
【請求項４】　請求項１ないし３のいずれか１項に記載のコンテンツ暗号化方法において、
各分割部分に対して用いられた暗号鍵の集合の中から、各分割部分ごとに１つずつ暗号鍵を選択することで、暗号化されたコンテンツの復号に用いられる鍵束を生成する過程を備えることを、
特徴とするコンテンツ暗号化方法。
【請求項５】　コンテンツに電子透かし情報を埋め込んで暗号化するコンテンツ暗号化装置において、
コンテンツを複数の部分に分割する手段と、
上記分割した部分の全て又は一部を処理対象として、処理対象の分割部分のそれぞれに対して、複数の異なる電子透かし情報を埋め込む手段と、
上記電子透かし情報の埋め込まれた分割部分及びその埋め込みの行われなかった分割部分を、別々の暗号鍵を使って暗号化する手段とを備えることを、
特徴とするコンテンツ暗号化装置。
【請求項６】　全て又は一部の分割部分のそれぞれに対して複数の異なる電子透かし情報が埋め込まれるとともに、その埋め込みの行われた分割部分及びその埋め込みの行われなかった分割部分が別々の暗号鍵を使って暗号化されることで生成される暗号化コンテンツの集合を復号対象として、暗号化コンテンツを復号するコンテンツ復号方法であって、
各分割部分に対して用いられた暗号鍵の集合の中から、各分割部分ごとに１つずつ暗号鍵が選択されることで構成される鍵束の１つを取得する過程と、
上記鍵束を構成する各暗号鍵に対応付けられる暗号化コンテンツ部分を取り出す過程と、
上記取り出した暗号化コンテンツ部分を、それに対応付けられる暗号鍵で復号する過程と、
上記復号したコンテンツ部分を統合することでコンテンツを復元する過程とを備えることを、
特徴とするコンテンツ復号方法。
【請求項７】　全て又は一部の分割部分のそれぞれに対して複数の異なる電子透かし情報が埋め込まれるとともに、その埋め込みの行われた分割部分及びその埋め込みの行われなかった分割部分が別々の暗号鍵を使って暗号化されることで生成される暗号化コンテンツの集合を復号対象として、暗号化コンテンツを復号するコンテンツ復号装置であって、
各分割部分に対して用いられた暗号鍵の集合の中から、各分割部分ごとに１つずつ暗号鍵が選択されることで構成される鍵束の１つを取得する手段と、
上記鍵束を構成する各暗号鍵に対応付けられる暗号化コンテンツ部分を取り出す手段と、
上記取り出した暗号化コンテンツ部分を、それに対応付けられる暗号鍵で復号する手段と、
上記復号したコンテンツ部分を統合することでコンテンツを復元する手段とを備えることを、
特徴とするコンテンツ復号装置。
【請求項８】　電子透かし情報の埋め込まれた暗号化コンテンツを配布するコンテンツ配布方法において、
コンテンツを複数の部分に分割する過程と、
上記分割した部分の全て又は一部を処理対象として、処理対象の分割部分のそれぞれに対して、複数の異なる電子透かし情報を埋め込む過程と、
上記電子透かし情報の埋め込まれた分割部分及びその埋め込みの行われなかった分割部分を、別々の暗号鍵を使って暗号化する過程と、
各分割部分に対して用いられた暗号鍵の集合の中から、各分割部分ごとに１つずつ暗号鍵を選択することで構成される鍵束を生成する過程と、
上記暗号化した分割部分の集合で構成される暗号化コンテンツを全ての配布先に配布する過程と、
上記鍵束を１つ選択して、その選択した上記鍵束の暗号化したものを配布先に配布する過程とを備えることを、
特徴とするコンテンツ配布方法。
【請求項９】　請求項８に記載のコンテンツ配布方法において、
配布先と、その配布先に配布した上記鍵束との対応関係を配布記録として記録するか、配布先と、その配布先に配布した上記鍵束により復号されるコンテンツから読み出される電子透かし情報との対応関係を配布記録として記録する過程を備えることを、
特徴とするコンテンツ配布方法。
【請求項１０】　請求項８又は９に記載のコンテンツ配

布方法において、
上記鍵束と、それにより復号されるコンテンツから読み出される電子透かし情報との対応関係のリストを生成する過程を備えることを、
特徴とするコンテンツ配布方法。
【請求項１１】　請求項８又は９に記載のコンテンツ配布方法において、
コンテンツに埋め込まれるべき電子透かし情報が与えられるときに、規定の変換に従って、その埋め込みを実現する上記鍵束を求めることで、上記鍵束と、それにより復号されるコンテンツから読み出される電子透かし情報との対応関係を動的に特定する過程を備えることを、
特徴とするコンテンツ配布方法。
【請求項１２】　請求項１０又は１１に記載のコンテンツ配布方法において、
上記鍵束を配布する過程では、配布先ＩＤから求められる電子透かし情報を選択し、上記対応関係に従って、その電子透かし情報に対応付けられる上記鍵束を選択して、それを配布先に配布するように処理することを、
特徴とするコンテンツ配布方法。
【請求項１３】　請求項１０又は１１に記載のコンテンツ配布方法において、
上記鍵束を配布する過程では、未発行の電子透かし情報を選択し、上記対応関係に従って、その電子透かし情報に対応付けられる上記鍵束を選択して、それを配布先に配布するように処理することを、
特徴とするコンテンツ配布方法。
【請求項１４】　電子透かし情報の埋め込まれた暗号化コンテンツを配布するコンテンツ配布装置において、
コンテンツを複数の部分に分割する手段と、
上記分割した部分の全て又は一部を処理対象として、処理対象の分割部分のそれぞれに対して、複数の異なる電子透かし情報を埋め込む手段と、
上記電子透かし情報の埋め込まれた分割部分及びその埋め込みの行われなかった分割部分を、別々の暗号鍵を使って暗号化する手段と、
各分割部分に対して用いられた暗号鍵の集合の中から、各分割部分ごとに１つずつ暗号鍵を選択することで構成される鍵束を生成する手段と、
上記暗号化した分割部分の集合で構成される暗号化コンテンツを全ての配布先に配布する手段と、
上記鍵束を１つ選択して、その選択した上記鍵束の暗号化したものを配布先に配布する手段とを備えることを、
特徴とするコンテンツ配布装置。
【請求項１５】　全て又は一部の分割部分のそれぞれに対して複数の異なる電子透かし情報が埋め込まれるとともに、その埋め込みの行われた分割部分及びその埋め込みの行われなかった分割部分が別々の暗号鍵を使って暗号化されて配布され、更に、各分割部分ごとに１つずつ該暗号鍵が選択されることで構成される鍵束を使って復号されるコンテンツを検査対象として、コンテンツの違法コピーを検査するコンテンツ違法コピー検査方法であって、
検査対象のコンテンツに埋め込まれる電子透かし情報を読み取る過程と、
上記読み取った電子透かし情報をキーにして、コンテンツの配布先ユーザと、その配布先ユーザに配布された上記鍵束により復号されるコンテンツから読み出される電子透かし情報との対応関係について記述するリストを参照することで、検査対象のコンテンツの正規の配布先ユーザを特定する過程と、
上記特定した正規の配布先ユーザと、検査対象のコンテンツを所有するユーザとが一致するのか否かを検査する過程とを備えることを、
特徴とするコンテンツ違法コピー検査方法。
【請求項１６】　全て又は一部の分割部分のそれぞれに対して複数の異なる電子透かし情報が埋め込まれるとともに、その埋め込みの行われた分割部分及びその埋め込みの行われなかった分割部分が別々の暗号鍵を使って暗号化されて配布され、更に、各分割部分ごとに１つずつ該暗号鍵が選択されることで構成される鍵束を使って復号されるコンテンツを検査対象として、コンテンツの違法コピーを検査するコンテンツ違法コピー検査方法であって、
検査対象のコンテンツに埋め込まれる電子透かし情報を読み取る過程と、
上記読み取った電子透かし情報の埋め込みを実現する上記鍵束を特定する過程と、
上記特定した鍵束をキーにして、コンテンツの配布先ユーザと、その配布先ユーザに配布された上記鍵束との対応関係について記述するリストを参照することで、検査対象のコンテンツの正規の配布先ユーザを特定する過程と、
上記特定した正規の配布先ユーザと、検査対象のコンテンツを所有するユーザとが一致するのか否かを検査する過程とを備えることを、
特徴とするコンテンツ違法コピー検査方法。
【請求項１７】　全て又は一部の分割部分のそれぞれに対して複数の異なる電子透かし情報が埋め込まれるとともに、その埋め込みの行われた分割部分及びその埋め込みの行われなかった分割部分が別々の暗号鍵を使って暗号化されて配布され、更に、各分割部分ごとに１つずつ該暗号鍵が選択されることで構成される鍵束を使って復号されるコンテンツを検査対象として、コンテンツの違法コピーを検査するコンテンツ違法コピー検査装置であって、
検査対象のコンテンツに埋め込まれる電子透かし情報を読み取る手段と、
上記読み取った電子透かし情報をキーにして、コンテンツの配布先ユーザと、その配布先ユーザに配布された上

記鍵束により復号されるコンテンツから読み出される電子透かし情報との対応関係について記述するリストを参照することで、検査対象のコンテンツの正規の配布先ユーザを特定する手段と、
上記特定した正規の配布先ユーザと、検査対象のコンテンツを所有するユーザとが一致するのか否かを検査する手段とを備えることを、
特徴とするコンテンツ違法コピー検査装置。
【請求項１８】　全て又は一部の分割部分のそれぞれに対して複数の異なる電子透かし情報が埋め込まれるとともに、その埋め込みの行われた分割部分及びその埋め込みの行われなかった分割部分が別々の暗号鍵を使って暗号化されて配布され、更に、各分割部分ごとに１つずつ該暗号鍵が選択されることで構成される鍵束を使って復号されるコンテンツを検査対象として、コンテンツの違法コピーを検査するコンテンツ違法コピー検査装置であって、
検査対象のコンテンツに埋め込まれる電子透かし情報を読み取る手段と、
上記読み取った電子透かし情報の埋め込みを実現する上記鍵束を特定する手段と、
上記特定した鍵束をキーにして、コンテンツの配布先ユーザと、その配布先ユーザに配布された上記鍵束との対応関係について記述するリストを参照することで、検査対象のコンテンツの正規の配布先ユーザを特定する手段と、
上記特定した正規の配布先ユーザと、検査対象のコンテンツを所有するユーザとが一致するのか否かを検査する手段とを備えることを、
特徴とするコンテンツ違法コピー検査装置。
【請求項１９】　請求項１ないし４のいずれか１項に記載のコンテンツ暗号化方法の実現に用いられる処理をコンピュータに実行させるためのコンテンツ暗号化プログラム。
【請求項２０】　請求項１ないし４のいずれか１項に記載のコンテンツ暗号化方法の実現に用いられる処理をコンピュータに実行させるためのプログラムを記録したコンテンツ暗号化プログラムの記録媒体。
【請求項２１】　請求項６に記載のコンテンツ復号方法の実現に用いられる処理をコンピュータに実行させるためのコンテンツ復号プログラム。
【請求項２２】　請求項６に記載のコンテンツ復号方法の実現に用いられる処理をコンピュータに実行させるためのプログラムを記録したコンテンツ復号プログラムの記録媒体。
【請求項２３】　請求項８ないし１３のいずれか１項に記載のコンテンツ配布方法の実現に用いられる処理をコンピュータに実行させるためのコンテンツ配布プログラム。
【請求項２４】　請求項８ないし１３のいずれか１項に記載のコンテンツ配布方法の実現に用いられる処理をコンピュータに実行させるためのプログラムを記録したコンテンツ配布プログラムの記録媒体。
【請求項２５】　請求項１５又は１６に記載のコンテンツ違法コピー検査方法の実現に用いられる処理をコンピュータに実行させるためのコンテンツ違法コピー検査プログラム。
【請求項２６】　請求項１５又は１６に記載のコンテンツ違法コピー検査方法の実現に用いられる処理をコンピュータに実行させるためのプログラムを記録したコンテンツ違法コピー検査プログラムの記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、コンテンツに電子透かし情報を埋め込んで暗号化するコンテンツ暗号化方法及び装置と、その暗号化技術により暗号化されたコンテンツを復号するコンテンツ復号方法及び装置と、その暗号化技術により暗号化されたコンテンツを配布するコンテンツ配布方法及び装置と、その暗号化技術により暗号化されたコンテンツの違法コピーを検査するコンテンツ違法コピー検査方法及び装置と、そのコンテンツ暗号化方法の実現に用いられるコンテンツ暗号化プログラム及びそのプログラムを記録した記録媒体と、そのコンテンツ復号方法の実現に用いられるコンテンツ復号プログラム及びそのプログラムを記録した記録媒体と、そのコンテンツ配布方法の実現に用いられるコンテンツ配布プログラム及びそのプログラムの記録媒体と、そのコンテンツ違法コピー検査方法の実現に用いられるコンテンツ違法コピー検査プログラム及びそのプログラムを記録した記録媒体とに関する。
【０００２】
【従来の技術】ディジタルデータは劣化なくコピーが作成可能で、ネットワークを用いた再配布が容易という特徴をもつ。これへの対策として用いられるのが電子透かしである。電子透かしは、画像や音声などのコンテンツに人間の視覚や聴覚では認識困難な形で別の情報を埋め込む手法である。
【０００３】電子透かしのコンテンツ保護への利用法のひとつは、コンテンツの著作権に関わる情報を埋め込む方式である。これはコンテンツの著者名や識別子を電子透かしで埋め込み、コピー流布時に、この情報によって正当な権利の主張を可能にするものである。
【０００４】しかしながら、この著作権に関わる情報の埋め込みによる保護は、電子透かしから違法コピーを行ったものに関する情報は得られず、違法コピー対策の効果は弱い。
【０００５】第２の電子透かし利用法は、電子透かしとしてコンテンツの利用者に関する情報を埋め込むものである。これはコンテンツを利用者に販売または譲渡した場合に、その利用者の情報がコンテンツに電子透かしと

して埋め込まれるようにする。

【０００６】この場合、違法コピーされたコンテンツに埋め込まれた電子透かしの情報から、コンテンツが当初販売または譲渡されたユーザが識別可能となり、違法コピーの流出経路に関する情報が得られるため、違法コピー対策が著作権に関わる情報を埋め込む場合より高い。

【０００７】一方、著作権情報を埋め込む場合には、同一コンテンツに埋め込むべき電子透かし情報は唯一であるため、同一電子透かしを埋め込まれたデータの大量コピーを配布することが可能である。

【０００８】これに対して、利用者情報を埋め込む場合には、同一コンテンツに埋め込む場合であっても電子透かし情報は配布先の利用者ごとに異なり、配布先ごとに新たなコンテンツデータを生成する必要がある。これはコンテンツ提供者にとって非常に負荷が大きいのみならず、ＣＤ－ＲＯＭや放送といったコンテンツの一括の大量流通が不可能となるという問題を発生させる。

【０００９】本出願人が開示した特開平10-191025 号に記載される発明では、これを解決するために、電子透かしの埋め込みを利用者側で行う方法を提案している。

【００１０】この発明では、コンテンツをスクランブルして利用者に送付し、これとは別に、スクランブル解除鍵と電子透かしとして埋め込む利用者情報とを合成したデータを利用者に送付する。利用者はコンテンツを利用する場合にスクランブルを解除するが、スクランブル解除器には電子透かし埋め込み機能を持たせており、スクランブル解除鍵と同時に、送付した利用者情報を電子透かしを使ってスクランブルを解除したコンテンツに埋めこむ。

【００１１】これによって電子透かしの埋め込みをコンテンツ利用者に行わせることが可能となり、コンテンツ提供者の負荷を低減させるとともに、ＣＤ－ＲＯＭや放送によるコンテンツ配布との両立を可能にしている。

【００１２】

【発明が解決しようとする課題】しかしながら、この方式（特開平10-191025 号に記載される発明の方式）では、スクランブル解除と透かし埋め込みの二つの処理から構成されるため、スクランブル解除を行う処理のみを不正に抽出された場合、電子透かしの埋め込まれていないコンテンツが生成される危険性がある。

【００１３】また、この方式では、利用者に送付される情報の中に透かしとして埋め込まれるべき情報が含まれるため、送付された利用者情報が電子透かしとして埋め込まれる前の段階で改ざんされた場合、偽の利用者情報がコンテンツに埋め込まれる可能性がある。

【００１４】本発明は、このような問題を解決するためのものであり、利用者情報の電子透かしとしてのコンテンツへの埋め込みを利用者側で効率よく行いながら、利用者側で電子透かし情報の埋め込みを不正にキャンセルしたり、偽の電子透かし情報が埋め込まれることを防止できるようにする新たな電子透かし情報の埋め込み技術の提供を目的とする。

【００１５】

【課題を解決するための手段】図１に、本発明を具備するシステム構成の一例を図示する。

【００１６】図中、１は本発明を具備するコンテンツプロバイダ、２-ｉ（ｉ＝１～ｎ）は本発明を具備するユーザ端末、３は本発明を具備するコンテンツ違法コピー検査機関である。

【００１７】本発明を具備するコンテンツプロバイダ１は、本発明のコンテンツ暗号化装置１０と本発明のコンテンツ配布装置１１とを備え、本発明を具備するユーザ端末２-ｉは、本発明のコンテンツ復号装置２０を備え、本発明を具備するコンテンツ違法コピー検査機関３は、本発明のコンテンツ違法コピー検査装置３０を備える。

【００１８】（１）コンテンツ暗号化装置１０の構成

本発明のコンテンツ暗号化装置１０は、暗号化対象のコンテンツを処理対象として、①コンテンツを複数の部分に分割する手段と、②その分割した部分の全て又は一部を処理対象として、処理対象の分割部分のそれぞれに対して、複数の異なる電子透かし情報を埋め込む手段と、③電子透かし情報の埋め込まれた分割部分及びその埋め込みの行われなかった分割部分を、別々の暗号鍵を使って暗号化する手段と、④各分割部分に対して用いられた暗号鍵の集合の中から、各分割部分ごとに１つずつ暗号鍵を選択することで、暗号化されたコンテンツの復号に用いられる鍵束を生成する手段とを備えるように構成する。

【００１９】（２）コンテンツ復号装置２０の構成

本発明のコンテンツ復号装置２０は、本発明のコンテンツ暗号化装置１０が生成した暗号化コンテンツの集合を復号対象として、①本発明のコンテンツ暗号化装置１０が生成した鍵束の１つを取得する手段と、②その取得した鍵束を構成する各暗号鍵に対応付けられる暗号化コンテンツ部分を取り出す手段と、③その取り出した暗号化コンテンツ部分を、それに対応付けられる暗号鍵で復号する手段と、④その復号したコンテンツ部分を統合することでコンテンツを復元する手段とを備えるように構成する。

【００２０】ここで、本発明のコンテンツ復号装置２０は、コンテンツプロバイダ１から配布されてくる鍵束が暗号化されていることに対応して、それを復号する手段を備えることになる。

【００２１】（３）コンテンツ配布装置１１の構成

本発明のコンテンツ配布装置１１は、本発明のコンテンツ暗号化装置１０が生成した暗号化コンテンツの集合を配布対象として、本発明のコンテンツ暗号化装置１０が備えられる場合には、①本発明のコンテンツ暗号化装置１０が生成した暗号化コンテンツの集合を全ての配布先に配布する手段と、②本発明のコンテンツ暗号化装置１

０が生成した鍵束を１つ選択して、その選択した鍵束の暗号化したものを配布先に配布する手段とを備える。一方、本発明のコンテンツ暗号化装置１０が備えられない場合には、この２つの手段の他に、本発明のコンテンツ暗号化装置１０の備える各手段を備えるように構成する。

【００２２】更に、本発明のコンテンツ配布装置１１は、③配布先と、その配布先に配布した鍵束との対応関係を配布記録として記録するか、配布先と、その配布先に配布した鍵束により復号されるコンテンツから読み出される電子透かし情報との対応関係を配布記録として記録する手段を備えたり、④鍵束と、それにより復号されるコンテンツから読み出される電子透かし情報との対応関係のリストを生成する手段を備えたり、⑤コンテンツに埋め込まれるべき電子透かし情報が与えられるときに、規定の変換に従って、その埋め込みを実現する鍵束を求めることで、鍵束と、それにより復号されるコンテンツから読み出される電子透かし情報との対応関係を動的に特定する手段を備えることがある。

【００２３】（４）コンテンツ違法コピー検査装置３０の構成

本発明のコンテンツ違法コピー検査装置３０は、本発明のコンテンツ復号装置２０が復号したコンテンツを検査対象として、①検査対象のコンテンツに埋め込まれる電子透かし情報を読み取る手段と、②その読み取った電子透かし情報をキーにして、本発明のコンテンツ配布装置１１が配布記録として記録した対応関係のリスト（コンテンツの配布先ユーザと、その配布先ユーザに配布した鍵束により復号されるコンテンツから読み出される電子透かし情報との対応関係のリスト）を参照することで、検査対象のコンテンツの正規の配布先ユーザを特定する手段と、③その特定した正規の配布先ユーザと、検査対象のコンテンツを所有するユーザとが一致するのか否かを検査する手段とを備えるように構成する。

【００２４】ここで、リストを参照する手段は、本発明のコンテンツ配布装置１１からそのリストを取得して参照することもあるし、本発明のコンテンツ配布装置１１に問い合わせることでそのリストを参照することもある。

【００２５】また、本発明のコンテンツ違法コピー検査装置３０は、本発明のコンテンツ復号装置２０が復号したコンテンツを検査対象として、①検査対象のコンテンツに埋め込まれる電子透かし情報を読み取る手段と、②規定の変換を施したり、本発明のコンテンツ配布装置１１が生成した対応関係のリスト（鍵束と、それにより復号されるコンテンツから読み出される電子透かし情報との対応関係のリスト）を参照することにより、その読み取った電子透かし情報の埋め込みを実現する鍵束を特定する手段と、③その特定した鍵束をキーにして、本発明のコンテンツ配布装置１１が配布記録として記録した対応関係のリスト（コンテンツの配布先ユーザと、その配布先ユーザに配布した鍵束との対応関係のリスト）参照することで、検査対象のコンテンツの正規の配布先ユーザを特定する手段と、④その特定した正規の配布先ユーザと、検査対象のコンテンツを所有するユーザとが一致するのか否かを検査する手段とを備えるように構成する。

【００２６】ここで、リストを参照する手段は、本発明のコンテンツ配布装置１１からそのリストを取得して参照することもあるし、本発明のコンテンツ配布装置１１に問い合わせることでそのリストを参照することもある。

【００２７】このように構成される本発明のコンテンツ配布装置１１（本発明のコンテンツ暗号化装置１０）では、例えば、図２に示すように、コンテンツｃをＬ個の（$c_1, c_2, \ldots, c_L$）に分割して、そのＬ個の各分割部分c_iに対して、例えば、電子透かし操作$w_{i,j}$（ｉは分割部分の識別子、ｊは埋め込む電子透かし情報の識別子）を使って電子透かし情報“０”，“１”を埋め込んでから、暗号鍵$k_{i,j}$（ｉは分割部分の識別子、ｊは電子透かし情報の識別子）を使って暗号化することで、それらの暗号化コンテンツの集合で構成されるコンテンツ配布用データを生成するとともに、それらの暗号鍵$k_{i,j}$から、Ｌ個の各分割部分c_iごとに１つずつ暗号鍵$k_{i,j}$を選択することで、コンテンツｃの復号に用いられる鍵束K_j（$j=1\sim 2^L$）を生成する。

【００２８】このとき、本発明のコンテンツ配布装置１１は、鍵束K_jと、それにより復号されるコンテンツから読み出される電子透かし情報d_j（図２の例では“０”と“１”の羅列データ）との対応関係のリストを生成する。

【００２９】続いて、本発明のコンテンツ配布装置１１は、図３に示すように、全てのユーザ端末2-i（図３の例では８台のユーザ端末）に対して、生成したコンテンツ配布用データを配布するとともに、各ユーザ端末2-iに対して、１つずつ鍵束K_jを選択して、その選択した鍵束K_jの暗号化したものを配布する。

【００３０】この鍵束K_jの選択処理は、例えば、配布先ユーザのＩＤから求められる電子透かし情報（例えば、ＩＤの２進数表現に対応付けられる電子透かし情報d_j）を選択し、生成してある鍵束K_jと電子透かし情報d_jとの対応関係のリストに従って、その電子透かし情報に対応付けられる鍵束を選択することで行ったり、未発行の電子透かし情報を選択し、生成してある鍵束K_jと電子透かし情報d_jとの対応関係のリストに従って、その電子透かし情報に対応付けられる鍵束を選択することで行う。

【００３１】ここで、鍵束K_jと電子透かし情報d_jとの対応関係のリストを予め生成しておかずに、電子透かし情報d_jが与えられるときに、規定の変換に従って、

その電子透かし情報ｄｊの埋め込みを実現する鍵束Ｋｊを動的に特定するようにしてもよい。例えば、“00000000”という電子透かし情報ｄｊが与えられるときには、図２の例で説明するならば、“０”が８個並ぶことで、その電子透かし情報ｄｊの埋め込みを実現する鍵束Ｋｊは、

$K_j = k_{1,1}, k_{2,1}, k_{3,1}, \cdots\cdots, k_{L,1}$

であるというように、その時点で、与えられた電子透かし情報ｄｊに対応付けられる鍵束Ｋｊを動的に特定するようにしてもよいのである。

【００３２】このような配布処理を行うときに、本発明のコンテンツ配布装置１１は、本発明のコンテンツ違法コピー検査装置３０によるコンテンツ違法コピー検査を可能ならしめるために、図３に示すように、その配布記録として、配布先ユーザのＩＤと、その配布先ユーザに配布した鍵束Ｋｊとの対応関係を記録したり、配布先ユーザのＩＤと、その配布先ユーザに配布した鍵束Ｋｊにより復号されるコンテンツから読み出される電子透かし情報ｄｊ（図３の例では“０”と“１”の羅列データ）との対応関係を記録する。

【００３３】一方、本発明のコンテンツ復号装置２０は、本発明のコンテンツ配布装置１１から配布される鍵束を受けて、受信してあるコンテンツ配布用データから、その鍵束を構成する各暗号鍵に対応付けられる暗号化コンテンツ部分を取り出し、その取り出した暗号化コンテンツ部分を、それに対応付けられる暗号鍵で復号して、その復号したコンテンツ部分を統合することでコンテンツを復元する。

【００３４】このようにして復元されるコンテンツには、配布される鍵束に従って、配布先ユーザに固有な電子透かし情報が埋め込まれることになる。しかも、この配布先ユーザに固有な電子透かし情報の埋め込みは、配布先のユーザ側で行われることになる。

【００３５】一方、本発明のコンテンツ違法コピー検査装置３０は、検査対象のコンテンツが与えられると、そのコンテンツに埋め込まれる電子透かし情報を読み取り、それをキーにして、本発明のコンテンツ配布装置１１が記録した配布記録のリスト（コンテンツの配布先ユーザと、その配布先ユーザに配布された鍵束により復号されるコンテンツから読み出される電子透かし情報との対応関係のリスト）を参照することで、検査対象のコンテンツの正規の配布先ユーザを特定して、それに従って、検査対象のコンテンツを所有するユーザが正規のコンテンツ所有者であるのかを検査する。

【００３６】また、本発明のコンテンツ違法コピー検査装置３０では、検査対象のコンテンツが与えられると、そのコンテンツに埋め込まれる電子透かし情報を読み取り、規定の変換を施すことなどにより、その読み取った電子透かし情報の埋め込みを実現する鍵束を特定して、それをキーにして、本発明のコンテンツ配布装置１１が記録した配布記録のリスト（コンテンツの配布先ユーザと、その配布先ユーザに配布された鍵束との対応関係のリスト）を参照することで、検査対象のコンテンツの正規の配布先ユーザを特定して、それに従って、検査対象のコンテンツを所有するユーザが正規のコンテンツ所有者であるのかを検査する。

【００３７】このようにして検査されるコンテンツには、正規のコンテンツ所有者に固有の電子透かし情報が埋め込まれており、これにより、コンテンツ所有者が正規の所有者であるのか否かということと、コンテンツの不正コピーが行われた場合には、どの正規のコンテンツ所有者の所有するコンテンツからコピーが行われたのかということを検出できるようになる。

【００３８】このようにして、本発明では、ユーザ側で、ユーザに固有な電子透かし情報をコンテンツに埋め込むという形態をとりつつ、そのとき埋め込む電子透かし情報とその埋め込み処理とについては、実際には鍵束を使って提供側で制御するようにしており、これにより、ユーザ側で、電子透かし情報の埋め込みを不正にキャンセルしたり、偽の電子透かし情報が埋め込まれることを防止できるようになる。

【００３９】そして、コンテンツの不正コピーが行われる場合に、それを正確に検出できるとともに、そのコピー元を正確に検出できるようになる。

【００４０】以上に説明したように、本発明では、コンテンツを複数の部分に分割して、それぞれの分割部分に対して複数の電子透かしを用意し、個々のユーザに対する電子透かしを、抽出された分割部分の電子透かしの値の組み合わせとするという構成を採っており、これにより、電子透かし入りコンテンツとして用意すべきデータ量を少なくできるようになる。

【００４１】すなわち、従来行われていたように、コンテンツに直接、利用者情報を電子透かしとして埋めこむ場合、ｎ人の利用者に対してはｎ通りに電子透かしを埋めこむ必要があり、提供者での電子透かし埋め込み回数はｎ回となる。元のコンテンツのデータ量をＣとすると、電子透かしによるデータ量増加がないと仮定しても、電子透かし入りコンテンツのデータ量の合計はＣ×ｎである。これでは、利用者が増加するにつれて、膨大な埋め込み回数になるとともに、膨大なデータ量になる。

【００４２】このように、従来技術に従っていると、電子透かし埋め込み回数の問題から、提供者の負荷が大きく、また、データ量の問題から、予め用意したコンテンツのＣＤ－ＲＯＭや放送などによる一括の配布が不可能となっている。

【００４３】これに対して本発明の方式では、コンテンツからｍ個の部分を抽出し、各部分にｋ種類の電子透かしデータを対応させる場合、コンテンツ全体でk^m種類の電子透かしが埋め込める。ｎ人の利用者に対しては、

およそ、「ｋ×log ｎ÷lonｋ」回の電子透かし埋め込みとなり、ｎに比べて非常に少ない。また、ｎ人の利用者すべてを区別する電子透かしの組み合わせを実現するためのデータ量も、これに比例するため、Ｃ×ｎに比べて非常に少ない。

【００４４】さらに、抽出部分の合計Ｃ’（本発明の電子透かし埋め込み処理の対象となる部分の合計）をコンテンツのデータ量Ｃに比べて小さくとると、異なる利用者のための電子透かしを埋め込んだデータを予め用意するためのデータ量が「Ｃ’×log ｎ÷lon ｋ」となり、オリジナルコンテンツＣに比べてｎ人の利用者用の電子透かし情報追加のためのデータ量が小さく、予め全利用者用の電子透かし入りコンテンツを用意してＣＤ－ＲＯＭなどによる一括配布や、放送やサーバからのダウンロードによる一括配布などが可能となる。

【００４５】

【発明の実施の形態】以下、実施の形態に従って本発明を詳細に説明する。

【００４６】本発明の説明に入る前に、数学的な準備を行う。

【００４７】コンテンツの符号化の形式Ｆに対して、次のような性質を満たす分割操作Ωとその逆変換とを用意する。ここでいう形式Ｆとは、画像符号化におけるビットマップ符号化やＪＰＥＧ、動画符号化におけるＭＰＥＧ、音声符号化におけるＭＰ３などをさす。

【００４８】（１）［性質Ω：Ωの性質］

形式Ｆで符号化されたコンテンツｃは、分割操作Ωによって複数（Ｌ個）の部分$c_1, c_2, \ldots, c_L$に分割される。これをＣ＝Ω（ｃ）と書くことにする。ここで、Ｃは分割部分の系列で、$C = c_1, c_2, \ldots, c_L$である。

【００４９】分割操作Ωは、その逆変換Ω’（結合操作と呼ぶ）が定義できて、Ω’を分割された部分の系列$C = c_1, c_2, \ldots, c_L$に適用することによって、形式Ｆを満たすコンテンツｃ’を生成できる。これをｃ’＝Ω’（Ｃ）またはｃ’＝Ω’（$c_1, c_2, \ldots, c_L$）と書くことにする。（この性質の説明終了）。

【００５０】次に、形式Ｆ、操作Ωに対して、以下のような性質を満たす、コンテンツの分割部分に対する操作（電子透かし操作になる）の集合の系列

$W = v_1, v_2, \ldots, v_L$

但し、$v_i = (w_{i,1}, w_{i,2}, \ldots, w_{i,Ni})$,（ｉ＝１～Ｌ）

を用意する。

【００５１】（２）［性質Ｗ１：Ｗの性質］

Ωによって行われるコンテンツの分割によるｉ番目（ｉ＝1, 2, ..., L）の分割部分のそれぞれに対して、操作の集合v_iを対応させる。Ωによるコンテンツｃのｉ番目の分割部分c_iに、v_i中の任意の操作$w_{i,k}$を適用することで得られたデータを$w_{i,k}$（c_i）とする。

【００５２】ここで、v_i（ｉ＝1, 2, ..., L）の中から、各ｉに対して任意の操作$w_{i,k}$を一つずつ選んで、各分割部分に対する操作の系列からなる「分割部分の系列に対する操作」

$w = w_{1,k1}, w_{2,k2}, \ldots, w_{L,kL}$

を作り、これを分割部分の系列Ｃに次のように適用する。

【００５３】$w(C) = w_{1,k1}(c_1), w_{2,k2}(c_2), \ldots\ldots, w_{L,kL}(c_L)$

このとき、これにΩ’を適用することで得られたデータ

$c^w = \Omega'(w(C)) = \Omega'(w_{1,k1}(c_1), w_{2,k2}(c_2), \ldots\ldots, w_{L,kL}(c_L))$

は、もとのコンテンツｃが符号化形式Ｆを満足していれば、ふたたびＦを満足する。（この性質の説明終了）。

【００５４】符号化Ｆを満足するあるコンテンツｃと分割操作Ωに対して、Ｗが次のような性質を満足するとき、Ｗはｃに識別子を埋め込むと呼ぶことにし、Ｗ中の操作をそれぞれの対象への識別子埋め込み操作と呼ぶ。

【００５５】（３）［性質Ｗ２：Ｗの性質］

Ｗから取った、分割部分の系列に対する二つの操作w_1, w_2

$w_1 = w_{1,k1}, w_{2,k2}, \ldots, w_{L,kL}$

$w_2 = w_{1,m1}, w_{2,m2}, \ldots, w_{L,mL}$

が一致しない、つまり、w_1, w_2中のある分割部分に対する操作$w_{j,kj}$と$w_{j,mj}$とが異なる場合には、ｃを分割してw_1とw_2とを適用して統合すると、異なったコンテンツデータが得られる。つまり、

$\Omega'(w_1(\Omega(c))) \neq \Omega'(w_2(\Omega(c)))$

となる。（この性質の説明終了）。

【００５６】次に、識別子埋め込み操作Ｗに対して、以下のような二つの性質を満たす、コンテンツからのデータの読み取り操作Ｒ（電子透かしの読み取り操作になる）を用意する。

【００５７】（４）［性質Ｒ１：Ｒの性質］

一つのＷからとられた任意の二つの異なる、分割部分の系列に対する異なる操作w_1とw_2とに対して、

$R(\Omega'(w_1(\Omega(c)))) \neq R(\Omega'(w_2(\Omega(c))))$

が成立し、また、任意の分割部分の系列に対する操作ｗに対して

$R(c) \neq R(\Omega'(w(\Omega(c))))$

が成立する。ここで、Ｒ（ｃ）は、データを読み取れない（Ｒ（ｃ）＝φ、読み取りエラー）場合を含む。（この性質の説明終了）。

【００５８】（５）［性質Ｒ２：Ｒによるデータのコンテンツに独立な読み取り］

あるＷから取られた分割部分の系列に対する操作ｗと、形式Ｆを満たす異なるコンテンツｃａ，ｃｂとが存在したとき

$R(\Omega'(w(\Omega(ca)))) = R(\Omega'(w(\Omega(cb))))$

となる。

【００５９】すなわち、異なるコンテンツに同一の電子

透かし情報が埋め込まれた場合に、コンテンツからのデータの読み取り操作Ｒを施すことで、同一の電子透かし情報を読み出せることになる。（この性質の説明終了）。

【００６０】コンテンツｃにデータ読み取り操作Ｒを適用することで、あるデータｄ＝Ｒ（ｃ）が抽出できる。ここで、分割部分の系列に対する識別子埋め込み操作ｗのとり方は「$N_1 \times N_2 \times \cdots \times N_L$」種類ある。これから、操作$\Omega'(w(\Omega(c)))$によって、Ｒから読み出されるデータが異なるものとなる「$N_1 \times N_2 \times \cdots \times N_L$」個のコンテンツが得られることを示す。

【００６１】また、Ｒが［性質Ｒ２］を満足するとき、ｗが同一であればコンテンツに関わらず同一のデータが読み出せることになる。（準備終了）。

【００６２】以上のような準備のもとに、コンテンツの安全な配布について実現する本発明の一実施形態例について説明する。

【００６３】ここで、以下の説明では、説明の便宜上、コンテンツに埋め込む電子透かし情報として、識別子のような目に見えるような情報を想定しているが、本発明はそのような電子透かし情報の埋め込みに限られるものではなくて、要するに、性質の異なるものをコンテンツに埋め込むことで構成される電子透かしに対して、そのまま適用できる。また、コンテンツも画像に限られるものでもない。

【００６４】図４に、図１に示した本発明を具備するコンテンツプロバイダ１及びユーザ端末２の持つ機能構成の一実施形態例を図示し、図５に、図１に示した本発明を具備するコンテンツ違法コピー検査機関３の持つ機能構成の一実施形態例を図示する。

【００６５】本発明を具備するコンテンツプロバイダ１は、図４に示すように、ユーザ端末２へコンテンツを送信するための暗号化されたコンテンツ配布用データを生成するコンテンツ配布用データ生成部１００と、生成されたコンテンツ配布用データを保存するコンテンツ配布用データ格納部１０１と、保存されるコンテンツ配布用データをユーザ端末２に送信するコンテンツ配布用データ送信部１０２と、コンテンツ配布用データの復号に用いられる鍵束を生成する鍵束生成部１０３と、生成された鍵束とそれにより復号されるコンテンツから読み出される識別子（ユーザに固有な電子透かし情報）との対応関係を管理する鍵束識別子対応リスト１０４と、コンテンツに埋め込まれるべき識別子が与えられるときに、その埋め込みを実現する鍵束を動的に特定する識別子鍵束変換部１０５と、ユーザ端末２に送信する送信先に固有の鍵束を選択する鍵束選択部１０６と、選択された鍵束を暗号化してユーザ端末２に送信する鍵束送信部１０７と、ユーザ端末２に送信した鍵束の情報（ユーザＩＤと、送信した鍵束と、その鍵束により復号されるコンテンツから読み出される識別子との対応関係の情報）を保存する配布記録格納部１０８とを備える。

【００６６】ここで、このコンテンツ配布用データ生成部１００やコンテンツ配布用データ送信部１０２や鍵束生成部１０３や識別子鍵束変換部１０５や鍵束選択部１０６や鍵束送信部１０７は、具体的にはコンピュータプログラムで実現されるものであり、これらのコンピュータプログラムは、計算機が読み取り可能な半導体メモリなどの適当な記録媒体に格納することができる。

【００６７】一方、本発明を具備するユーザ端末２は、図４に示すように、コンテンツプロバイダ１から送信されてくるコンテンツ配布用データを受信するコンテンツ配布用データ受信部２００と、受信されたコンテンツ配布用データを保存するコンテンツ配布用データ格納部２０１と、コンテンツプロバイダ１から送信されてくる暗号化された鍵束を受信して復号する鍵束受信部２０２と、受信された鍵束を使って、受信されたコンテンツ配布用データを復号することでコンテンツを復元するコンテンツ復元部２０３とを備える。

【００６８】ここで、このコンテンツ配布用データ受信部２００や鍵束受信部２０２やコンテンツ復元部２０３は、具体的にはコンピュータプログラムで実現されるものであり、これらのコンピュータプログラムは、計算機が読み取り可能な半導体メモリなどの適当な記録媒体に格納することができる。

【００６９】一方、本発明を具備するコンテンツ違法コピー検査機関３は、図５に示すように、検査対象のコンテンツに埋め込まれる識別子（ユーザに固有な電子透かし情報）を読み出す識別子読出部３００と、コンテンツプロバイダ１の持つ配布記録格納部１０８の情報を取得する取得部３０１と、取得された配布記録格納部１０８の情報（ユーザＩＤと識別子との対応関係の情報）を保存する配布記録格納部３０２と、取得された配布記録格納部１０８の情報（ユーザＩＤと鍵束との対応関係の情報）を保存する配布記録格納部３０３と、規定の変換を施したり、本発明を具備するコンテンツプロバイダ１が生成した鍵束識別子対応リスト１０４の情報を参照することで、検査対象のコンテンツから読み出された識別子に対応付けられる鍵束を特定する鍵束特定部３０４と、配布記録格納部３０２の情報を参照しつつ検査対象のコンテンツが違法コピーされたものであるのか否かを検査する違法コピー検査部３０５と、配布記録格納部３０３の情報を参照しつつ検査対象のコンテンツが違法コピーされたものであるのか否かを検査する違法コピー検査部３０６とを備える。

【００７０】ここで、識別子読出部３００や取得部３０１や鍵束特定部３０４や違法コピー検査部３０５や違法コピー検査部３０６は、具体的にはコンピュータプログラムで実現されるものであり、これらのコンピュータプログラムは、計算機が読み取り可能な半導体メモリなどの適当な記録媒体に格納することができる。

【００７１】なお、この実施形態例では、コンテンツプロバイダ１からユーザ端末２にダウンロードすることでコンテンツを配布するという構成を採っているが、コンテンツの配布方法としては、放送やサーバなどからのダウンロードによる配布の他に、ＣＤ－ＲＯＭなどを使って配布する方法など様々なものがあり、本発明はそれらの配布方法に対して適用可能である。

【００７２】（ｉ）コンテンツプロバイダ１の処理の説明

（イ）コンテンツ配布用データ生成部１００の処理

コンテンツ配布用データ生成部１００は、図６の処理フローを実行することで、利用者へコンテンツを配布するためのコンテンツ配布用データを生成する処理を行う。

【００７３】すなわち、先ず最初に、形式Ｆで符号化された配布対象となるコンテンツｃに対して分割操作Ωを施し、コンテンツの分割部分の系列Ｃ＝$c_1, c_2, \ldots, c_L$を生成する。

【００７４】続いて、識別子埋め込み操作の集合Ｗを用意し、Ｗ内の各々の持つ分割部分に対する識別子埋め込み操作$w_{i,j}$を、Ｃの対応する分割部分c_iに適用して、$N_1 + N_1 + \cdots + N_L$個の分割部分

$w_{1,1}(c_1)$, $w_{1,2}(c_1)$, ..., $w_{1,N1}(c_1)$,

$w_{2,1}(c_2)$, $w_{2,2}(c_2)$, ..., $w_{2,N2}(c_2)$,

.....,

$w_{L,1}(c_L)$, $w_{L,2}(c_L)$, ..., $w_{L,NL}(c_L)$

を生成する。

【００７５】続いて、識別子の埋め込まれた$N_1 + N_1 + \cdots + N_L$個の分割部分のそれぞれについて、別々の暗号鍵を用いて暗号化を行う。

【００７６】これによって得られた$N_1 + N_1 + \cdots + N_L$個の暗号化された分割部分の集まり、

$D = E(k_{1,1}, w_{1,1}(c_1)), E(k_{1,2}, w_{1,2}(c_1)), \ldots,$
$E(k_{1,N1}, w_{1,N1}(c_1)), E(k_{2,1}, w_{2,1}(c_2)), E(k_{2,2}, w_{2,2}(c_2)), \ldots, E(k_{2,N2}, w_{2,N2}(c_2)), \ldots, E(k_{L,1}, w_{L,1}(c_L)), E(k_{L,2}, w_{L,2}(c_L)), \ldots, E(k_{L,NL}, w_{L,NL}(c_L))$

をコンテンツ配布用データとする。

【００７７】ここで、$k_{i,j}$は暗号鍵を示し、Ｅ（ｋ，...）は暗号鍵ｋによる暗号化を示しており、したがって、Ｅ（$k_{i,j}$，$w_{i,j}$（c_i））はＣの分割部分c_iに識別子を埋め込んで暗号化したデータを示している。

【００７８】この暗号鍵の集合$k_i = \{k_{i,1}, k_{i,2}, \ldots, k_{i,Ni}\}$は、分割部分$c_i$に識別子を埋め込んで暗号化したデータに対する復号鍵の集合となる。これから、暗号鍵の集合k_iを単に分割部分c_iに対する鍵集合と呼ぶことにする。

【００７９】最後に、この生成したコンテンツ配布用データをコンテンツ配布用データ格納部１０１に格納する。

【００８０】この処理を実行するにあたって、コンテンツ配布用データ生成部１００は、分割操作Ωによってコンテンツｃを（Ｌ個）の部分$c_1, c_2, \ldots, c_L$に分割するときに、部分c_1を主体部、それ以外の部分$c_2, \ldots, c_L$を調整部というように、それらの分割部分を性質の異なる二種類のクラスに分けて、主体部については識別子埋め込み操作を行わないように処理してもよい。

【００８１】つまり、分割部分に対する操作集合において、$v_1 = (w_{1,1}) = (I)$（Ｉは恒等変換）とすることで、主体部のc_1に対しては操作を施さないように処理してもよい。このとき、$c_2, \ldots, c_L$のデータ量をc_1のデータ量に比べて少なくとるように処理してもよい。

【００８２】すなわち、コンテンツｃの全ての部分に対して、本発明による識別子の埋め込み操作を行う必要はなく、また、電子透かしの埋め込みが難しいコンテンツ部分もあるので、例えば、そのようなコンテンツ部分を主体部として、その部分に対しては本発明による識別子埋め込み操作を行わないように処理するのである。

【００８３】また、本発明による識別子の埋め込み操作を行うと、それに応じてコンテンツ配布用データのデータ量が大きくなるので、それを防止するために、このように主体部を設けて、主体部については本発明による識別子埋め込み操作を行わないように処理するのである。

【００８４】この主体部について、本発明による識別子の埋め込み操作を行わないという構成を採るのではなくて、固定的な識別子の埋め込み操作を行うように処理してもよい。

【００８５】つまり、分割部分に対する操作集合において、$v_1 = (w_{1,1}$（１つしか識別子埋め込み操作を用意しない））とすることで、c_1に対しては固定的操作を施すように処理してもよい。このときにも、$c_2, \ldots, c_L$のデータ量をc_1のデータ量に比べて少なくとるように処理してもよい。

【００８６】識別子を埋め込まないよりは、固定的なものであっても識別子を埋め込んだ方が好ましいので、コンテンツ配布用データのデータ量の削減を図りつつ、主体部について、固定的な識別子の埋め込み操作を行うように処理するのである。

【００８７】（ロ）コンテンツ配布用データ送信部１０２の処理

コンテンツ配布用データ送信部１０２は、コンテンツ配布用データ格納部１０１に格納されるコンテンツ配布用データを全てのユーザ端末２に送信する処理を行う。すなわち、全てのユーザ端末２に対して、同じコンテンツ配布用データを送信する処理を行う。

【００８８】（ハ）鍵束生成部１０３の処理

鍵束生成部１０３は、図７の処理フローを実行することで、コンテンツの復号に用いられる鍵束を生成する処理を行う。

【００８９】すなわち、先ず最初に、コンテンツ配布用データ生成部１００から、コンテンツ配布用データの生成に用いられた各分割部分c_iに対する鍵集合k_iを取得する。

【００９０】続いて、その取得した鍵集合k_iからひとつ鍵$k_{i,ji}$を選択することを各c_iについて繰り返すことで、$N_1 \times N_1 \times \cdots \times N_L$個の鍵束$K_j$

$K_j = k_{1,j1}, k_{2,j2}, \ldots, k_{L,jL}$

を作成する。ここで、j_iはiごとに異なる数である。

【００９１】最後に、各鍵束ごとに、それにより埋め込まれる識別子d_jを求めることで、鍵束と識別子との対応関係について記述する鍵束識別子対応リスト１０４を生成する。図２に例示するように、鍵束と識別子との対応関係を求めて、それに基づいて鍵束識別子対応リスト１０４を生成するのである。

【００９２】このようにして生成される鍵束K_jは、Ωによるcの各分割部分に識別子埋め込みと暗号化を行うことによって得られたデータに対する鍵を一つずつ含む。よって、鍵束K_jによって、cの各分割部分に対してある識別子を埋め込んだものの復号された形のデータが一つずつ得られることになる。

【００９３】なお、管理情報として必要であれば、鍵束には、鍵束K_j中の各鍵がコンテンツcのどの分割部分に対応するのかを示す鍵の対応情報を付属させる。鍵と分割部分との対応は、例えば、鍵束中の鍵に順序をつけ、これを分割部分の順序を対応させるといった手段をとることができる。

【００９４】このようにして、鍵束の構成、つまり鍵束に含まれる鍵の構成によって、cの全分割部分に埋め込まれた識別子の総体として得られる、復元されたコンテンツc'の識別子の値が決定されることになる。

【００９５】次に、鍵束識別子対応リスト１０４の生成処理について説明する。

【００９６】鍵束K_jによって埋め込まれるデータをd_jとする。つまり

$d_j = R(\Omega'(w_j(\Omega(c))))$

とする。ここで、w_jはK_jに対応した識別子埋め込み操作である。

【００９７】鍵束生成部１０３は、この対応関係に従って、各鍵束K_jに対して埋め込まれた識別子d_jを求め、その対応関係（K_j，d_j）のリストを生成することで、鍵束識別子対応リスト１０４を生成する。

【００９８】（ニ）識別子鍵束変換部１０５の処理

後述するように、鍵束選択部１０６は、コンテンツに埋め込む識別子を選択し、鍵束識別子対応リスト１０４を参照することで、その識別子に対応付けられる鍵束を選択していくように処理する。

【００９９】この処理のために、鍵束識別子対応リスト１０４が鍵束生成部１０３により生成されることになるが、この鍵束識別子対応リスト１０４が生成されない場合には、識別子鍵束変換部１０５は、鍵束選択部１０６が選択した鍵束に対応付けられる鍵束を動的に特定する処理を行う。

【０１００】埋め込まれる識別子がｄであるとする。ここで、ｄの値の決定に、鍵束中の各鍵によって暗号化されたコンテンツの分割部分に埋め込まれた情報が独立に影響する場合、つまり、ｄの値から、それ自身以外の分割部分に埋め込まれた値に独立した形で、各分割部分に埋め込まれたデータを決定できる場合には、ｉ番目の部分に埋め込まれた識別子d_iは、ある関数Fd_iによって、

$d_i = Fd_i(d)$

として求められる。このFd_iは操作Ｒから求める。

【０１０１】最も簡単な例で説明するならば、コンテンツｃが４つに分割され、各分割部分に対して識別子０，１を埋め込んで暗号化する場合にあって、ｄ＝０１０１が与えられると、識別子鍵束変換部１０５は、そのｄ＝０１０１に対応付けられる鍵束が分割部分c_1に識別子０を埋め込み、分割部分c_2に識別子１を埋め込み、分割部分c_3に識別子０を埋め込み、分割部分c_4に識別子１を埋め込む鍵束であると特定する処理を行うのである。

【０１０２】（ホ）鍵束選択部１０６の処理

鍵束選択部１０６は、あるユーザＵに対してコンテンツを配信する場合、図８（ａ）（ｂ）の処理フローに従って、別に送信するコンテンツ配布用データＤの復号に用いる鍵束をユーザごとに選択する処理を行う。

【０１０３】すなわち、図８（ａ）の処理フローに従う場合には、各ユーザに対して事前にユーザＩＤ（ｕで表す）を発行しておくとともに、ｕから流通コンテンツ識別子ｄへの変換を行う関数F_{user}（ｕ）を用意しておいて、ユーザ端末２から、その発行したユーザＩＤを指定して鍵束の送信要求が発行されると、先ず最初に、そのユーザＩＤをその関数F_{user}に代入することで、コンテンツに埋め込むべき識別子を求める。ここで、ｕとｄを同じ体系にしておけばｄ＝ｕとなり、関数F_{user}を省略できる。

【０１０４】続いて、鍵束識別子対応対応リスト１０４を参照することで、その識別子ｄに対応付けられる鍵束Ｋを選択する。このとき、識別子鍵束変換部１０５に変換依頼を発行することで、その識別子ｄに対応付けられる鍵束Ｋを特定するように処理することもある。

【０１０５】この選択した鍵束が鍵束送信部１０７により鍵束送信要求発行元のユーザ端末２に送信されることになるので、続いて、選択した鍵束を鍵束送信部１０７に通知するとともに、後述するコンテンツ違法コピーの検査処理のために、鍵束送信先のユーザのＩＤ（ｕ）と、求めた識別子ｄと、選択した鍵束Ｋとの対応関係（ｕ，ｄ，Ｋ）を配布記録格納部１０８に保存する。

【０１０６】一方、図８（ｂ）の処理フローに従う場合

には、ユーザ端末２から鍵束の送信要求が発行されると、先ず最初に、そのユーザに対して未発行の識別子ｄを割り当てる。

【０１０７】続いて、鍵束識別子対応対応リスト１０４を参照することで、その識別子ｄに対応付けられる鍵束Ｋを選択する。このとき、識別子鍵束変換部１０５に変換依頼を発行することで、その識別子ｄに対応付けられる鍵束Ｋを特定するように処理することもある。

【０１０８】この選択した鍵束が鍵束送信部１０７により鍵束送信要求発行元のユーザ端末２に送信されることになるので、続いて、選択した鍵束を鍵束送信部１０７に通知するとともに、後述するコンテンツ違法コピーの検査処理のために、鍵束送信先のユーザのＩＤ（ｕ）と、割り当てた識別子ｄと、選択した鍵束Ｋとの対応関係（ｕ，ｄ，Ｋ）を配布記録格納部１０８に保存する。

【０１０９】なお、コンテンツ違法コピーの検査処理の方法によっては、（ｕ，ｄ，Ｋ）を配布記録格納部１０８に保存するのではなくて、（ｕ，ｄ）または（ｕ，Ｋ）を保存するように処理してもよい。また、このとき保存するユーザのＩＤ（ｕ）としては、数字列のようなものばかりでなく、メールアドレスなどの別のシステムからユーザに与えられたものを用いてもよい。

【０１１０】（ヘ）鍵束送信部１０７の処理

鍵束送信部１０７は、鍵束選択部１０６から通知される鍵束を暗号化して、鍵束要求発行元のユーザ端末２に送信する処理を行う。

【０１１１】コンテンツ配布用データが全てのユーザ端末２に一律に送信されるのと異なって、鍵束については、ユーザに固有なものとして、各ユーザ端末２に１つずつそれぞれ異なるものが送信されることになる。

【０１１２】（ii）ユーザ端末２の処理の説明

（イ）コンテンツ配布用データ受信部２００の処理

コンテンツ配布用データ受信部２００は、コンテンツプロバイダ１から送信されてくるコンテンツ配布用データを受信して、コンテンツ配布用データ格納部２０１に格納する処理を行う。

【０１１３】（ロ）鍵束受信部２０２は、コンテンツプロバイダ１から送信されてくる暗号化された鍵束を受信して、復号する処理を行う。

【０１１４】（ハ）コンテンツ復元部２０３の処理

コンテンツ復元部２０３は、図９の処理フローを実行することで、コンテンツプロバイダ１から送信されてきたコンテンツ配布用データからコンテンツを復元する処理を行う。

【０１１５】すなわち、コンテンツプロバイダ１からの鍵束K_j（鍵束受信部２０２により復号される）を受け取ると、コンテンツ配布用データ格納部２０１から、復号対象のコンテンツ配布用データを読み出す。

【０１１６】続いて、受け取った鍵束K_jから各分割部分c_iに対応する鍵$k_{i,ji}$を取り出すとともに、復号対象となるコンテンツ配布用データから、それらの各鍵$k_{i,ji}$に対応する暗号化された分割部分$E(k_{i,ji}, w_{i,ji}(c_i))$を取り出す。

【０１１７】続いて、各$E(k_{i,ji}, w_{i,ji}(c_i))$に対して、$k_{i,ji}$を適用して復号処理を行うことで$w_{i,ji}(c_i)$を復号する。

【０１１８】続いて、このようにして復号した$w_{i,ji}(c_i)$に対して結合操作Ω'を適用して、コンテンツc^w

$$c^w = \Omega'(w_{1,j1}(c_1), w_{2,j2}(c_2), \ldots, w_{L,jL}(c_L))$$

を復元する。

【０１１９】このとき復元されるコンテンツには、コンテンツプロバイダ１から送信されてきた鍵束により指定されるユーザに固有の識別子が電子透かしの形で埋め込まれることになる。

【０１２０】（iii）コンテンツ違法コピー検査機関３の処理の説明

（イ）識別子読出部３００の処理

識別子読出部３００は、検査対象となるコンテンツ（ユーザ端末２により復元されたコンテンツ）に埋め込まれている識別子を読み出す処理を行う。

【０１２１】（ロ）取得部３０１の処理

取得部３０１は、コンテンツプロバイダ１の持つ配布記録格納部１０８の情報を取得して、それに基づいて、配布記録格納部３０２に対して、ユーザＩＤ（ｕ）とそれに対応付けられる識別子ｄとの対応関係の情報を登録したり、配布記録格納部３０３に対して、ユーザＩＤ（ｕ）とそれに対応付けられる鍵束Ｋとの対応関係の情報を登録する処理を行う。

【０１２２】（ハ）鍵束特定部３０４の処理

鍵束特定部３０４は、コンテンツプロバイダ１の備える識別子鍵束変換部１０５と同様の処理を実行することで、検査対象のコンテンツから読み出された識別子に対応付けられる鍵束を検出したり、コンテンツプロバイダ１の備える鍵束識別子対応リスト１０４を参照することで、検査対象のコンテンツから読み出された識別子に対応付けられる鍵束を検出する処理を行う。

【０１２３】（ニ）違法コピー検査部３０５の処理

違法コピー検査部３０５は、検査対象のコンテンツが与えられると、図１０の処理フローを実行することで、検査対象のコンテンツが違法コピーされたものであるのか否かを検査して、その検査結果を出力する処理を行う。

【０１２４】すなわち、先ず最初に、検査対象のコンテンツを所有するユーザのＩＤを入力する。続いて、識別子読出部３００から、検査対象のコンテンツから読み出された識別子を受け取る。

【０１２５】続いて、その受け取った識別子をキーにして、配布記録格納部３０２（ユーザＩＤとそれに対応付けられる識別子ｄとの対応関係を管理）の情報を参照することで、検査対象のコンテンツの正規の所有者のユー

ザＩＤを特定する。

【０１２６】続いて、入力したユーザＩＤと、その特定した正規の所有者のユーザＩＤとが一致するのか否かを判断することで、違法コピーが行われたのか否かを検査して、その検査結果を出力する。

【０１２７】（ホ）違法コピー検査部３０６の処理

違法コピー検査部３０６は、検査対象のコンテンツが与えられると、図１１の処理フローを実行することで、検査対象のコンテンツが違法コピーされたものであるのか否かを検査して、その検査結果を出力する処理を行う。

【０１２８】すなわち、先ず最初に、検査対象のコンテンツを所有するユーザのＩＤを入力する。続いて、識別子読出部３００から読み出される識別子に応答して鍵束特定部３０４により特定される鍵束を、鍵束特定部３０４から受け取る。

【０１２９】続いて、その受け取った鍵束をキーにして、配布記録格納部３０３（ユーザＩＤとそれに対応付けられる鍵束Ｋとの対応関係を管理）の情報を参照することで、検査対象のコンテンツの正規の所有者のユーザＩＤを特定する。

【０１３０】続いて、入力したユーザＩＤと、その特定した正規の所有者のユーザＩＤとが一致するのか否かを判断することで、違法コピーが行われたのか否かを検査して、その検査結果を出力する。

【０１３１】このように構成される本発明について、その処理について具体的に説明すると、図２及び図３で説明したものとなる。

【０１３２】すなわち、本発明を具備するコンテンツプロバイダ１は、例えば、図２に示すように、コンテンツｃをＬ個の（$c_1, c_2, \ldots, c_L$）に分割して、そのＬ個の各分割部分c_iに対して、例えば、電子透かし操作$w_{i,j}$を使って識別子“０”，“１”を埋め込んでから、暗号鍵$k_{i,j}$を使って暗号化することで、それらの暗号化コンテンツの集合で構成されるコンテンツ配布用データを生成するとともに、それらの暗号鍵$k_{i,j}$から、Ｌ個の各分割部分c_iごとに１つずつ暗号鍵$k_{i,j}$を選択することで、コンテンツｃの復号に用いられる鍵束K_j（$j=1\sim 2^L$）を生成する。

【０１３３】このとき、本発明を具備するコンテンツプロバイダ１は、鍵束K_jと、それにより復号されるコンテンツから読み出される識別子d_j（図２の例では“０”か“１”の羅列データ）との対応関係について記述する鍵束識別子対応リスト１０４を生成する。

【０１３４】続いて、本発明を具備するコンテンツプロバイダ１は、図３に示すように、全てのユーザ端末２-ｉに対して、生成したコンテンツ配布用データを配布するとともに、各ユーザ端末２-ｉに対して、１つずつ鍵束K_jを選択して、その選択した鍵束K_jの暗号化したものを配布する。

【０１３５】この鍵束K_jの選択処理は、例えば、配布先ユーザのＩＤを関数F_{user}（ｕ）に代入することで識別子を得て、それをキーにして鍵束識別子対応リスト１０４を参照することで行ったり、未発行の識別子を選択し、それをキーにして鍵束識別子対応リスト１０４を参照することで行う。

【０１３６】ここで、鍵束識別子対応リスト１０４が生成されていないときには、識別子を指定して、識別子鍵束変換部１０５に対して変換依頼を発行することで、識別子に対応付けられる鍵束を得るように処理する。

【０１３７】このような配布処理を行うときに、本発明を具備するコンテンツプロバイダ１は、本発明を具備するコンテンツ違法コピー検査機関３によりコンテンツ違法コピー検査を可能ならしめるために、図３に示すように、その配布記録として、鍵束送信先のユーザのＩＤ（ｕ）と、割り当てた識別子ｄと、選択した鍵束Ｋとの対応関係（ｕ，ｄ，Ｋ）を配布記録格納部１０８に保存する。

【０１３８】一方、本発明を具備するユーザ端末２は、本発明を具備するコンテンツプロバイダ１から配布される鍵束を受けて、受信してあるコンテンツ配布用データから、その鍵束を構成する各暗号鍵に対応付けられる暗号化コンテンツ部分を取り出し、その取り出した暗号化コンテンツ部分を、それに対応付けられる暗号鍵（復号鍵）で復号して、その復号したコンテンツ部分を統合することでコンテンツを復元する。

【０１３９】このようにして復元されるコンテンツには、配布される鍵束に従って、配布先ユーザに固有な電子透かし情報が埋め込まれることになる。しかも、この配布先ユーザに固有の電子透かし情報の埋め込みは、配布先のユーザ側で行われることになる。

【０１４０】一方、本発明を具備するコンテンツ違法コピー検査機関３は、検査対象のコンテンツが与えられると、そのコンテンツに埋め込まれる識別子を読み取り、それをキーにして、本発明を具備するコンテンツプロバイダ１が保存する配布記録の情報を参照することで、検査対象のコンテンツの正規の配布先ユーザを特定して、それに従って、検査対象のコンテンツを所有するユーザが正規のコンテンツ所有者であるのかを検査する。

【０１４１】このようにして検査されるコンテンツには、正規のコンテンツ所有者に固有の識別子が埋め込まれており、これにより、コンテンツ所有者が正規の所有者であるのか否かということと、コンテンツの不正コピーが行われた場合には、どの正規のコンテンツ所有者の所有するコンテンツからコピーが行われたのかということを検出できるようになる。

【０１４２】このようにして、本発明では、ユーザ側で、ユーザに固有な電子透かし情報をコンテンツに埋め込むという形態をとりつつ、そのとき埋め込む電子透かし情報とその埋め込み処理とについては、実際には鍵束を使って提供側で制御するようにしており、これによ

り、ユーザ側で、電子透かし情報の埋め込みを不正にキャンセルしたり、偽の電子透かし情報が埋め込まれることを防止できるようになる。

【０１４３】そして、コンテンツの不正コピーが行われる場合に、それを正確に検出できるとともに、そのコピー元を正確に検出できるようになる。

【０１４４】

【実施例】（１）静止画像データに対するコンテンツ配布用データ生成

（イ）［分割操作Ω］

静止画像データを縦横ｎ×ｍの格子状に分割し、ｎ×ｍ個の部分を分割部分とする。この操作を分割操作Ωとする。

【０１４５】結合操作Ω’は、ｎ×ｍ個の部分を元の位置に並べて元のサイズの画像とするものである。この際に、符号化パラメータなどのヘッダ情報が符号化方式Ｆのデータに存在する場合は、各分割部分のデータにこの値を受け継ぎ、結合時にパラメータを復元する。

【０１４６】ＪＰＥＧ画像においては、８×８画素のブロックに分割して、ブロック毎に圧縮符号化が行われる。これから、格子状に分割する場合には、格子の縦横の画素数をブロックの画素数の倍数にして、画像をｎ’×ｍ’ブロックからなる矩形領域に分割する。

【０１４７】（ロ）［識別子埋め込み操作Ｗ］

各分割部分に対して、画像への電子透かし埋め込み方式を用いて識別子を埋め込む。電子透かし方式は埋め込みデータを指定することで、同一アルゴリズムで複数のデータの埋め込みが可能である。この操作を識別子埋め込み操作Ｗとする。

【０１４８】つまり、各$w_{i,j}$は、共通の透かしアルゴリズムｗによって、あるデータ$d_{i,j}$を電子透かしでコンテンツに埋め込む操作として実現する。$d_{i,j}$は$j \neq j'$のとき$d_{i,j} \neq d_{i,j'}$となるようにとる。読み取り関数ＲはＷから自然に定義される。

【０１４９】（ハ）［暗号化］

識別子を埋め込まれたコンテンツの分割部分に対して、実施形態例で説明したような暗号化を適用する。

【０１５０】（２）動画データに対するコンテンツ配布用データ生成

（イ）［分割操作Ω］

ＭＰＥＧ符号化された動画データにおいて、Ｐピクチャ、Ｂピクチャにおける動き補償ベクトルを符号化した部分をフレームごとに取り出し、最初のフレームから取り出したものを分割部分c_2、次のフレームから取り出したものを分割部分c_3というように、Ｌ－１個の調整部が存在する場合に、Ｌ－１フレーム周期で動き補償ベクトル符号化部分を分割部分に割り当てる。

【０１５１】また、元のコンテンツｃの符号化データから動き補償ベクトルを符号化した部分を取り除いたデータを主体部c_1とする。

【０１５２】結合操作Ω’は、Ωと逆に、主体部c_1から調整部を取り除いたのと逆の手続きで動き補償ベクトルをc_1に追加することで行う。

【０１５３】（ロ）［識別子埋め込み］

調整部c_kに割り当てられた動き補償ベクトルを、埋め込む値にしたがって変位を加える。

【０１５４】（ハ）［暗号化］

識別子を埋め込まれたコンテンツの分割部分に対して、実施形態例で説明したような暗号化を適用する。

【０１５５】（３）流通方式（会員登録あり）

コンテンツｃの所有者は、配布用コンテンツ作成および配布を行うためのセンタにコンテンツを預ける。

【０１５６】センタは、分割操作Ω、識別子埋め込み操作Ｗ、分割部分の暗号化を行ってコンテンツ配布用データＤを作成する。

【０１５７】センタは、コンテンツ配布用データＤを配布する。ここでの配布方式としては、ＣＤ－ＲＯＭに焼き付けて物流によって配送、インターネット上のデータサーバからのダウンロード、放送波による配信、電子メールによる配信など、任意のデータ配送手段を用いてよい。

【０１５８】ユーザは、配布されたコンテンツ配布用データＤを入手する。ユーザは、配布されたコンテンツ配布用データＤを復号して、コンテンツｃを復元するための鍵束をセンタに要求する。この要求時に、ユーザは、復号したいコンテンツと、センタに登録してあるユーザＩＤとをセンタに送信する。

【０１５９】センタは、ユーザＩＤに対応した鍵束Ｋを用意する。鍵束Ｋの用意の方法としては、実施形態例に述べた方法に基づいて行う。センタは、この用意した鍵束Ｋをユーザに送付する。

【０１６０】鍵束Ｋの送付については、一般的な鍵配送方式を用いる。これらの方式の一つとして、鍵束Ｋを配送用の鍵ｋで暗号化して送付する方式がある。別の方式としては、さらに鍵ｋをユーザの公開鍵k_uで暗号化して、鍵束Ｋに加えて鍵ｋをユーザに送付する方法がある。Infoket が鍵配送の代表的例である。

【０１６１】ユーザは、鍵束Ｋを受信し、実施形態例で説明した「コンテンツの復元法」に基づいて：コンテンツc^wを復元する。ここで、c^wは識別子を埋め込まれたコンテンツである。

【０１６２】（４）流通方式（会員登録なし）

コンテンツｃの所有者は、配布用コンテンツ作成および配布を行うためのセンタにコンテンツを預ける。

【０１６３】センタは、分割操作Ω、識別子埋め込み操作Ｗ、分割部分の暗号化を行ってコンテンツ配布用データＤを作成する。

【０１６４】センタは、コンテンツ配布用データＤを配布する。ここでの配布方式としては、ＣＤ－ＲＯＭに焼き付けて物流によって配送、インターネット上のデータ

サーバからのダウンロード、放送波による配信、電子メールによる配信など、任意のデータ配送手段を用いてよい。

【０１６５】ユーザは、配布されたコンテンツ配布用データＤを入手する。ユーザは、配布されたコンテンツ配布用データＤを復号して、コンテンツｃを復元するための鍵束をセンタに要求する。この要求時に、ユーザは、復号したいコンテンツと、センタの外部に存在する認証機関から入手した認証データとをセンタに送信する。

【０１６６】センタは、ユーザＩＤに対応した鍵束Ｋを用意する。鍵束Ｋの用意の方法としては、実施形態例に述べた方法に基づいて行う。センタは、この用意した鍵束Ｋをユーザに送付する。

【０１６７】ユーザは、鍵束Ｋを受信し、実施形態例で説明した「コンテンツの復元法」に基づいて、コンテンツc^wを復元する。ここで、c^wは識別子を埋め込まれたコンテンツである。

【０１６８】（５）静止画像の場合の例

（イ）データの作成

Ｎ×Ｍ画素の画像をｎ×ｍ個のブロックに分割し、$C_1, C_2, \ldots, C_{n*m}$とする。各$C_i$は、（Ｎ／ｎ）×（Ｍ／ｍ）画素のブロックである。

【０１６９】この（Ｎ／ｎ）×（Ｍ／ｍ）画素のブロックに対する電子透かし埋め込み$W_1, W_2, \ldots, W_x$を用意する。これは、ブロックに、それぞれ異なる値$w_1, w_2, \ldots, w_x$を埋め込む操作を行う。

【０１７０】W_jによって透かしを埋め込まれたブロックC_iを$W_j(C_i)$と書くことにすると、各C_iに対してすべてのW_jを適用することで、

$W_1(C_1), W_2(C_1), \ldots, W_x(C_1), W_2(C_2), \ldots, W_x(C_{n*m})$

というｘ×ｎ×ｍ個のデータができる。

【０１７１】これを、それぞれ異なる鍵$k_{i,j}$で暗号化して、

$E(k_{1,1}, W_1(C_1)), E(k_{2,1}, W_2(C_1)), \ldots, E(k_{x,n*m}, W_x(C_{n*m}))$

というｘ×ｎ×ｍ個のデータを作成し、これをＣＤ－ＲＯＭなどに格納して配送する。

【０１７２】（ロ）鍵の送信

コンテンツプロバイダは、$i = 1, 2, 3, \ldots, n \times m$のそれぞれについて、鍵$k_{ji,i}$を選択し、鍵束

$K = (k_{j1,1}, k_{j2,2}, \ldots, k_{jn*m,n*m})$

を作成する。

【０１７３】（ハ）復元

ユーザは、鍵束Ｋを受け取り、その受け取った鍵束Ｋ中の各鍵$k_{ji,i}$を使って、対応する暗号化された透かし入りブロック$E(k_{ji,i}, W_{ji}(C_i))$を復号することで、

$W_{j1}(C_1), W_{j2}(C_2), \ldots, W_{jn*m}(C_{n*m})$

を得て、それを統合することで画像を復元する。

【０１７４】これらのブロックを再構成してできたＮ×Ｍ画素の静止画像には、

$w_{j1}, w_{j2}, \ldots, w_{jn*m}$

というデータが透かしとして入っていることになる。

【０１７５】（６）違法コピー検査の効果

違法コピーを検査する機関は、検査対象となるコンテンツc^wに対し、データ読み取り操作Ｒを適用して識別子$d = R(c^w)$を取得する。

【０１７６】ここで、ｄは、コンテンツc^wの元となったコンテンツｃを配布したユーザを識別する情報となっている。

【０１７７】違法コピーを検査する機関は、センタで管理している識別子と鍵束との対応に基づき、読み出したデータｄから、コンテンツc^wの配布先のユーザＵを特定する。

【０１７８】コンテンツc^wを実際に所持していたユーザＵ’と、特定したユーザＵとが異なった場合、コンテンツc^wは最初の配布先とは異なるユーザに所持されていたことを示す。

【０１７９】この機能によって、あるユーザに所持されたコンテンツが違法コピーされたものかどうかを判断できるようになるとともに、違法コピーが元々どのユーザに配布されたものかを検出できる。

【０１８０】（７）透かしのチェック効果

本発明で配布されたコンテンツc^wに対する識別子の検査を次のように行うことで、透かしをチェックする。

【０１８１】コンテンツからのデータ読み取り操作Ｒによって、識別子$d = R(c^w)$を読み出す。

【０１８２】このｄは、鍵束Ｋ

$K_j = k_{1,j1}, k_{2,j2}, \ldots, k_{L,jL}$

に対応した透かし埋め込み操作

$w_j = w_{1,j1}, w_{2,j2}, \ldots, w_{L,jL}$

に一意に対応し、K_jの組み合わせが異なると、読み出されるデータｄは異なる。

【０１８３】よって、Ｒによって読み出されたｄから、どの鍵束が適用されてコンテンツが復元されたかが識別できる。

【０１８４】鍵束管理側では、鍵束Ｋまたは識別子ｄとユーザＵとの対応が管理されている。（Ｕ，ｄ）または（Ｕ，Ｋ）または（Ｕ，ｄ，Ｋ）が管理されている場合、ｄまたはＫからＵを知ることができる。

【０１８５】$d = F_{user}(u)$としてｄを決定した場合は、F_{user}の逆関数F_{user}^{-1}を用いてｄからｕを得ることができる。

【０１８６】これにより、あるユーザに所持されたコンテンツが違法コピーされたものかどうかを判断できるようになるとともに、違法コピーが元々どのユーザに配布されたものかを検出できる。

【０１８７】（８）データ量削減の効果

本発明では、コンテンツ配布用データに復号鍵を適用す

ることで得られる互いに異なる識別子をもつコンテンツは$N_1 \times N_2 \times \cdots \times N_L$種類生成される。

【０１８８】元のコンテンツのデータ量をｓ、分割部分$c_1, c_2, \ldots, c_L$のデータ量を$s_1, s_2, \ldots, s_L$とすると、ｃを分割せずに$N_1 \times N_2 \times \cdots \times N_L$種類の異なる識別子をもつコンテンツを生成する場合、合計のデータ量は、

$S = N_1 \times N_2 \times \cdots \times N_L \times s$

である。

【０１８９】これに対して、本発明による配布用データのサイズは、およそ

$S' = N_1 \times s_1 + N_2 \times s_2 + \cdots + N_L \times s_L$

である。

【０１９０】$s \fallingdotseq s_1 + s_2 + \cdots + s_L$であることから、$S \gg S'$となり、本発明によれば、非常に少ないデータ量で、多くの識別子を持ったコンテンツを同一の配布用データ内に用意できることになる。これは、ＣＤ－ＲＯＭなどによる同一コンテンツの大量流通に適している。

【０１９１】特に、N_kの値が大きいものほど、s_kを小さくとればＳ’はそれだけ小さくなる。

【０１９２】分割部分を主体部と調整部とにクラス分けした場合は、主体部のデータ量を多くとり、各調整部を少ないデータ量で構成される分割部分とすることで、このデータ削減効果は更に大きなものとなる。

【０１９３】図示実施形態例に従って本発明を説明したが、本発明はこれに限定されるものではない。例えば、実施形態例では、１つの電子透かし方式を使って、異なる電子透かし情報をコンテンツに埋め込むという構成を採ったが、コンテンツの分割部分毎に、その分割部分のコンテンツ属性に合った電子透かし方式を用いるという構成を用いることも可能である。

【０１９４】

【発明の効果】以上説明したように、本発明では、ユーザ側で、ユーザに固有な電子透かし情報をコンテンツに埋め込むという形態をとりつつ、そのとき埋め込む電子透かし情報とその埋め込み処理とについては、実際には鍵束を使って提供側で制御するようにしており、これにより、ユーザ側で、電子透かし情報の埋め込みを不正にキャンセルしたり、偽の電子透かし情報が埋め込まれることを防止できるようになる。

【０１９５】そして、コンテンツの不正コピーが行われる場合に、それを正確に検出できるとともに、そのコピー元を正確に検出できるようになる。

【０１９６】以上に説明したように、本発明では、コンテンツを複数の部分に分割して、それぞれの分割部分に対して複数の電子透かしを用意し、個々のユーザに対する電子透かしを、抽出された分割部分の電子透かしの値の組み合わせとするという構成を採っており、これにより、電子透かし入りコンテンツとして用意すべきデータ量を少なくできるようになる。

【０１９７】すなわち、従来行われていたように、コンテンツに直接、利用者情報を電子透かしとして埋めこむ場合、ｎ人の利用者に対してはｎ通りに電子透かしを埋めこむ必要があり、提供者での電子透かし埋め込み回数はｎ回となる。元のコンテンツのデータ量をＣとすると、電子透かしによるデータ量増加がないと仮定しても、電子透かし入りコンテンツのデータ量の合計はＣ×ｎである。これでは、利用者が増加するにつれて、膨大な埋め込み回数になるとともに、膨大なデータ量になる。

【０１９８】このように、従来技術に従っていると、電子透かし埋め込み回数の問題から、提供者の負荷が大きく、また、データ量の問題から、予め用意したコンテンツのＣＤ－ＲＯＭや放送などによる一括の配布が不可能となっている。

【０１９９】これに対して本発明の方式では、コンテンツからｍ個の部分を抽出し、各部分にｋ種類の電子透かしデータを対応させる場合、コンテンツ全体でk^m種類の電子透かしが埋め込める。ｎ人の利用者に対しては、およそ、「$k \times \log n \div \log k$」回の電子透かし埋め込みとなり、ｎに比べて非常に少ない。また、ｎ人の利用者すべてを区別する電子透かしの組み合わせを実現するためのデータ量も、これに比例するため、Ｃ×ｎに比べて非常に少ない。

【０２００】さらに、抽出部分の合計Ｃ’（本発明の電子透かし埋め込み処理の対象となる部分の合計）をコンテンツのデータ量Ｃに比べて小さくとると、異なる利用者のための電子透かしを埋め込んだデータを予め用意するためのデータ量が「$C' \times \log n \div \log k$」となり、オリジナルコンテンツＣに比べてｎ人の利用者用の電子透かし情報追加のためのデータ量が小さく、予め全利用者用の電子透かし入りコンテンツを用意してＣＤ－ＲＯＭなどによる一括配布や、放送やサーバからのダウンロードによる一括配布などが可能となる。

【図面の簡単な説明】

【図１】本発明を具備するシステムの構成の一例である。

【図２】本発明の処理の一例である。

【図３】本発明の処理の一例である。

【図４】本発明の一実施形態例である。

【図５】本発明の一実施形態例である。

【図６】コンテンツ配布用データ生成部の実行する処理フローの一実施形態例である。

【図７】鍵束生成部の実行する処理フローの一実施形態例である。

【図８】鍵束選択部の実行する処理フローの一実施形態例である。

【図９】コンテンツ復元部の実行する処理フローの一実施形態例である。

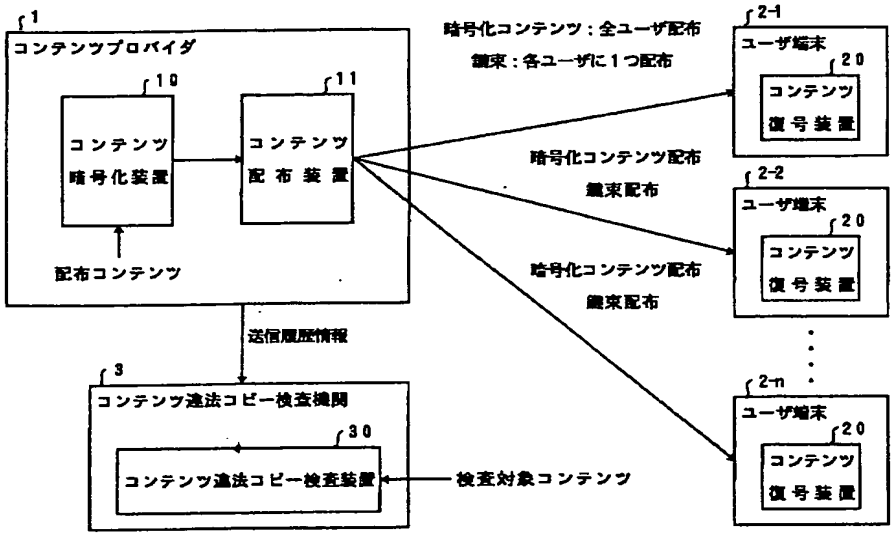
【図１０】違法コピー検査部の実行する処理フローの一実施形態例である。

【図１１】違法コピー検査部の実行する処理フローの一実施形態例である。

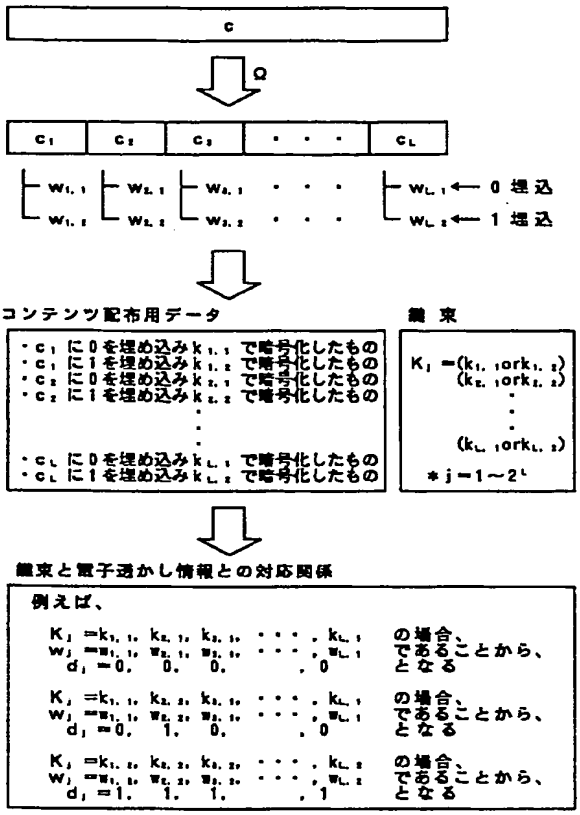
【符号の説明】

１	コンテンツプロバイダ
2-	ユーザ端末
３	コンテンツ違法コピー検査機関
１０	コンテンツ暗号化装置
１１	コンテンツ配布装置
２０	コンテンツ復号装置
３０	コンテンツ違法コピー検査装置
１００	コンテンツ配布用データ生成部
１０１	コンテンツ配布用データ格納部
１０２	コンテンツ配布用データ送信部
１０３	鍵束生成部
１０４	鍵束識別子対応リスト
１０５	識別子鍵束変換部
１０６	鍵束選択部
１０７	鍵束送信部
１０８	配布記録格納部
２００	コンテンツ配布用データ受信部
２０１	コンテンツ配布用データ格納部
２０２	鍵束受信部
２０３	コンテンツ復元部
３００	識別子読出部
３０１	取得部
３０２	配布記録格納部
３０３	配布記録格納部
３０４	鍵束特定部
３０５	違法コピー検査部
３０６	違法コピー検査部

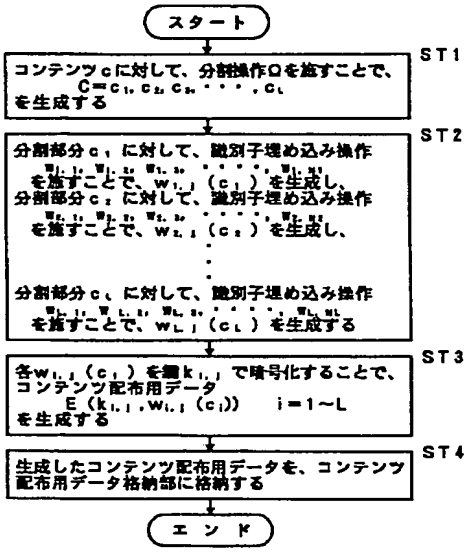
【図１】



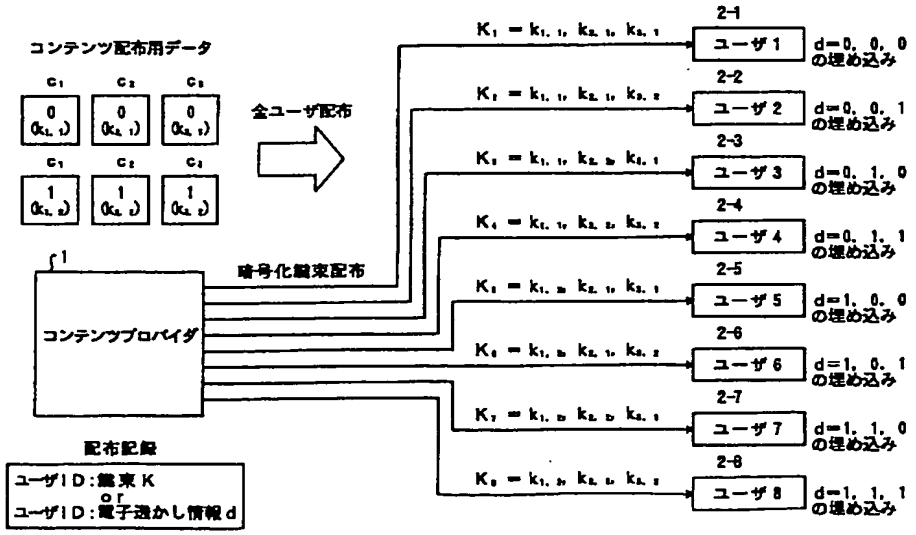
【図２】


c
Ω
c1 c2 c3 ・・・ cL
w1,1 w1,2 w2,1 w2,2 ・・・ wL,1 ← 0 埋込 wL,2 ← 1 埋込
コンテンツ配布用データ
・c1 に0を埋め込みk1,1で暗号化したもの
・c1 に1を埋め込みk1,2で暗号化したもの
・c2 に0を埋め込みk2,1で暗号化したもの
・c2 に1を埋め込みk2,2で暗号化したもの
・cL に0を埋め込みkL,1で暗号化したもの
・cL に1を埋め込みkL,2で暗号化したもの
鍵束
Kj =(k1,j or k1,2)
(k2,j or k2,2)
(kL,j or kL,2)
＊j=1～2^L
鍵束と電子透かし情報との対応関係
例えば、
Kj =k1,1, k2,1, k3,1, ・・・, kL,1 の場合、
wj =w1,1, w2,1, w3,1, ・・・, wL,1 であることから、
dj =0, 0, 0, , 0 となる
Kj =k1,1, k2,2, k3,1, ・・・, kL,1 の場合、
wj =w1,1, w2,2, w3,1, ・・・, wL,1 であることから、
dj =0, 1, 0, , 0 となる
Kj =k1,2, k2,2, k3,2, ・・・, kL,2 の場合、
wj =w1,1, w2,2, w3,2, ・・・, wL,2 であることから、
dj =1, 1, 1, , 1 となる

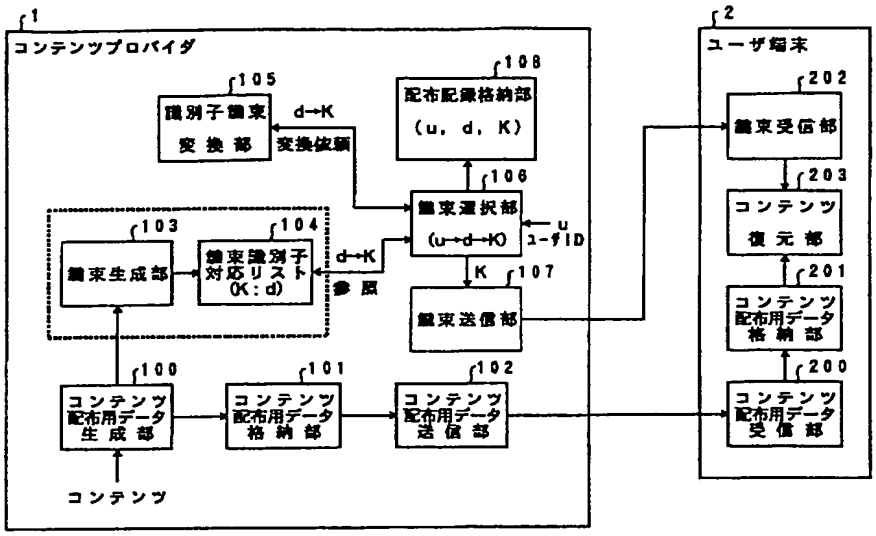
【図６】


スタート
コンテンツcに対して、分割操作Ωを施すことで、
C=c1, c2, c3, ・・・, cL
を生成する
ST1
分割部分c1に対して、識別子埋め込み操作
w1,1, w1,2, w1,3, ・・・, w1,2^L
を施すことで、w1,j (c1) を生成し、
分割部分c2に対して、識別子埋め込み操作
w2,1, w2,2, w2,3, ・・・, w2,2^L
を施すことで、w2,j (c2) を生成し、
・
・
・
分割部分cLに対して、識別子埋め込み操作
wL,1, wL,2, wL,3, ・・・, wL,2^L
を施すことで、wL,j (cL) を生成する
ST2
各w1,j (c1) を鍵k1,j で暗号化することで、
コンテンツ配布用データ
E (k1,j, w1,j (c1))　i=1～L
を生成する
ST3
生成したコンテンツ配布用データを、コンテンツ配布用データ格納部に格納する
ST4
エンド

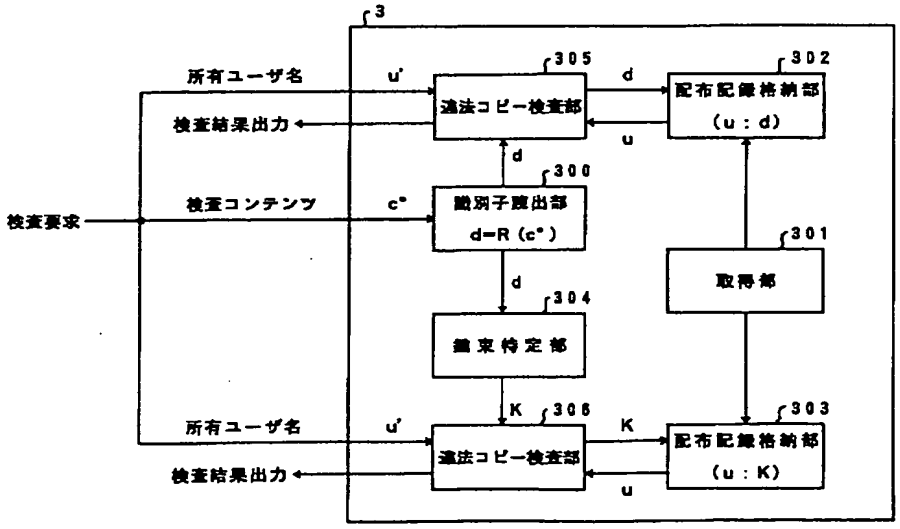
【図３】


コンテンツ配布用データ
c1 c2 c3
0 (k1,1) 0 (k2,1) 0 (k3,1)
1 (k1,2) 1 (k2,2) 1 (k3,2)
全ユーザ配布
暗号化鍵束配布
コンテンツプロバイダ
配布記録
ユーザID:鍵束K
or
ユーザID:電子透かし情報d
K1 = k1,1, k2,1, k3,1
K2 = k1,1, k2,1, k3,2
K3 = k1,1, k2,2, k3,1
K4 = k1,1, k2,2, k3,2
K5 = k1,2 k2,1, k3,1
K6 = k1,2 k2,1, k3,2
K7 = k1,2 k2,2 k3,1
K8 = k1,2 k2,2 k3,2
2-1 ユーザ1 d=0, 0, 0 の埋め込み
2-2 ユーザ2 d=0, 0, 1 の埋め込み
2-3 ユーザ3 d=0, 1, 0 の埋め込み
2-4 ユーザ4 d=0, 1, 1 の埋め込み
2-5 ユーザ5 d=1, 0, 0 の埋め込み
2-6 ユーザ6 d=1, 0, 1 の埋め込み
2-7 ユーザ7 d=1, 1, 0 の埋め込み
2-8 ユーザ8 d=1, 1, 1 の埋め込み

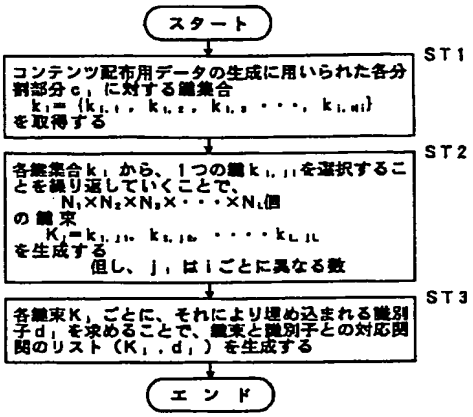
【図４】


1
コンテンツプロバイダ
105
識別子鍵束変換部
d→K
変換後鍵
108
配布記録格納部
(u, d, K)
106
鍵束選択部
(u→d→K)
u
ユーザID
103
鍵束生成部
104
鍵束識別子対応リスト
(K:d)
d→K
参照
K
107
鍵束送信部
100
コンテンツ配布用データ生成部
101
コンテンツ配布用データ格納部
102
コンテンツ配布用データ送信部
コンテンツ
2
ユーザ端末
202
鍵束受信部
203
コンテンツ復元部
201
コンテンツ配布用データ格納部
200
コンテンツ配布用データ受信部

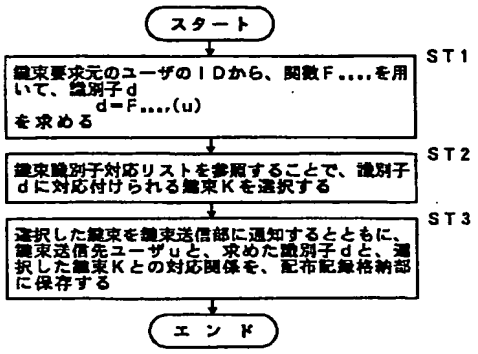
【図５】


3
所有ユーザ名
u'
305
違法コピー検査部
d
302
配布記録格納部
(u:d)
検査結果出力
u
d
検査要求
検査コンテンツ
c*
300
識別子抽出部
d=R(c*)
301
取得部
d
304
鍵束特定部
K
306
違法コピー検査部
K
303
配布記録格納部
(u:K)
所有ユーザ名
u'
検査結果出力
u

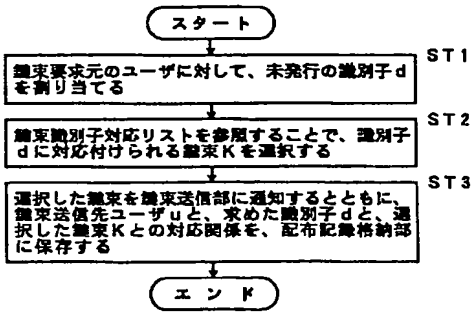
【図７】



【図８】

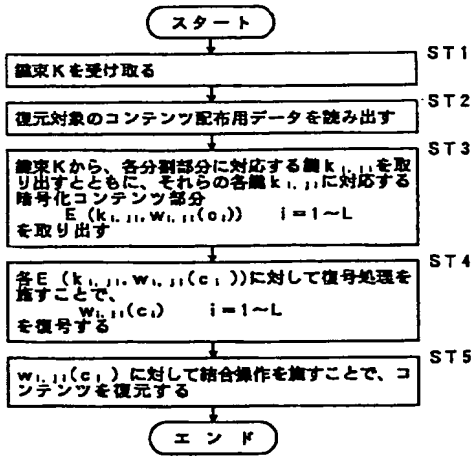


(a)

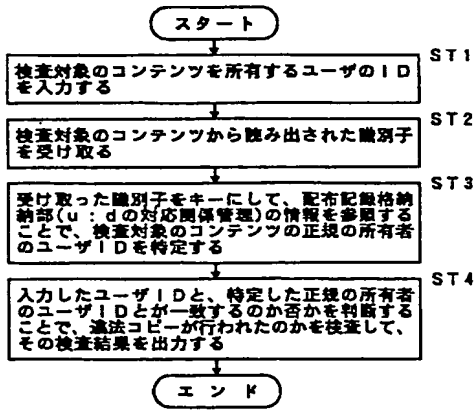


(b)

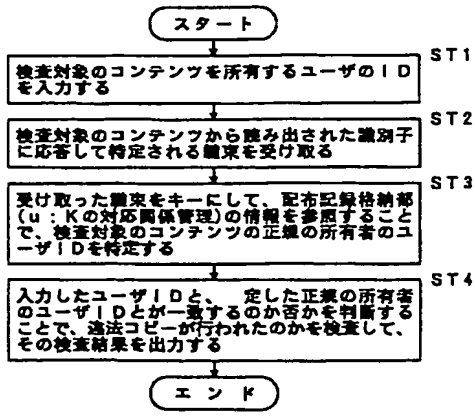
【図９】



【図１０】



【図１１】



フロントページの続き

(51) Int. Cl.[7]	識別記号	F I	ﾃｰﾏｺｰﾄﾞ（参考）
// Ｈ０４Ｎ 7/167			

Ｆターム(参考) 5C063 AB05 CA23 DA20 DB09
5C064 BA07 BB02 BB05 BC06 BC18
BC20 BC23 BD08 BD09
5J104 AA01 AA14 AA16 EA01 EA04
NA02

(54)【発明の名称】 コンテンツ暗号化方法及び装置と、コンテンツ復号方法及び装置と、コンテンツ配布方法及び装置と、コンテンツ違法コピー検査方法及び装置と、コンテンツ暗号化プログラム及びそのプログラムの記録媒体と、コンテンツ復号プログラム及びそのプログラムの記録媒体と、コンテンツ配布プログラム及びそのプログラムの記録媒体と、コンテンツ違法コピー検査プログラム及びそのプログラムの記録媒体